Points spéciaux et modularité des courbes elliptiques définies sur Q et Fq(t)

Valentin Petit

Points spéciaux et modularité des courbes elliptiques définies sur $\mathbb{Q}$ et $\mathbb{F}_q(T)$

Thèse de doctorat de
l'Université de Bourgogne Franche-Comté

École doctorale CARNOT-PASTEUR

présentée et soutenue publiquement le 25 mai 2023
en vue de l'obtention du grade de

Docteur de l'Université de Bourgogne Franche-Comté

(mention Mathématiques)

par

Valentin Petit

Composition du jury :

Bruno Anglès	Université Caen Normandie	*Rapporteur*
Emmanuel Royer	Université Clermont Auvergne	*Rapporteur*
Bill Allombert	CNRS – Université de Bordeaux	*Examinateur*
Sandra Rozensztajn	École Normale Supérieure de Lyon	*Examinatrice*
Cécile Armana	Université Bourgogne Franche-Comté	*Directrice de thèse*
Christophe Delaunay	Université Bourgogne Franche-Comté	*Directeur de thèse*

Table des matières

Remerciements

Je souhaiterais remercier dans un premier temps mes directeurs de thèses Cécile et Christophe d'avoir accepté de me prendre en thèse et de m'avoir accompagné depuis le début de mon Master 2. Ils ont été d'un grand soutient et de bons conseils notamment dans la rédaction de mes articles et de ma thèse. Ils ont su se montrer disponibles malgré les contextes difficiles et les lourdes tâches qui les incombent. Mais aussi pour leur patience face à mon anglais et mon orthographe désastreux.

Je tiens aussi à remercier Bruno Anglès et Emmanuel Royer d'avoir accepté d'être les rapporteurs de cette thèse. Un grand merci à Bill Allombert et Sandra Rozensztajn d'avoir accepté de faire partie des membres du jury.

J'adresse également mes remerciements à l'ensemble des membres du laboratoire de Mathématiques, pour leur accueil chaleureux et propice au travail. Je pense à toutes ces personnes qui ont été mes professeurs puis des collègues qui ont toujours été bienveillantes et qui m'ont permis d'en arriver là où j'en suis. Je tiens également à remercier Charlène, Claudia et Pascaline pour leur aide dans les démarches administrative, et dans l'organisation de divers évènements.

Un grand merci à l'équipe de théorie des nombres de m'avoir accueilli comme l'un des leurs. Je pense notamment à Jean-Robert et Olivier qui ont été souvent de bons conseils.

Je voudrais également remercié mes amis doctorants pour leur soutien, les bons moments partagés aux cours de ces années. Je pense à Mehdi, disparu au pays des caribous qui a essayé en vain de me convertir aux statistiques ; pas seulement collègue mais aussi grand adversaire de ping-pong et d'échec et partenaire de beuverie ; je pense aussi à Cécile, avec qui on a tant rigolé et qui a été un grand soutient au cours de ces années ; Une pensée également pour Marsault grand leader des groupes de travail et pour tous nos délires sur Bigard ; mais aussi à Yoël, Loris, Benjamin, Mathilde, Audrey, Florian,

Mathieu et tant d'autres.

Je remercie également mes amis de longue date Grégoire, Quentin, Nicolas, Julien et Théo pour leur soutient et tous ces bons moments partagés.

Mes derniers remerciements vont à ma famille, notamment à mes parents Nadine et Christian qui ont toujours cru en moi et qui m'ont toujours poussé à donner le meilleur de moi-même, mais également à mes deux sœurs Manon et Salomé qui m'ont soutenu tout au long de mes études.

Merci à tous.

Introduction

L'étude des courbes elliptiques trouve son origine et ses motivations dans des problèmes d'arithmétique très anciens. Il est bien connu que l'on peut munir une courbe elliptique d'une structure naturelle de groupe abélien que nous rappellerons dans la suite de cette introduction. L'objectif de cette thèse est d'étudier certains aspects explicites des courbes elliptiques. Nous allons nous intéresser à deux enjeux importants des courbes elliptiques : l'étude des points rationnels et l'étude de la modularité des courbes elliptiques. Nous allons étudier les courbes elliptiques dans deux cadres différents, la caractéristique 0 et la caractéristique positive.
Tout d'abord, nous nous intéressons à la non-divisibilité d'un point sur une famille de courbes elliptiques définies sur $\mathbb{Q}$ à deux paramètres. Cette famille est une généralisation de la famille de Washington et un cas particulier de la famille étudiée par Bettin, David et Delaunay. Le résultat obtenu généralise un résultat précédent de Duquesne. La démonstration de ce résultat fait appel à des propriétés arithmétiques de la famille et à des propriétés de la hauteur canonique.
Puis, dans le monde de la caractéristique positive nous nous intéressons à la paramétrisation modulaire des courbes elliptiques par les courbes modulaires de Drinfeld. Dans le contexte classique, les travaux de Wiles, Taylor, complétés par Breuil, Conrad, Diamond et Taylor montrent que toute courbe elliptique définie sur $\mathbb{Q}$ est modulaire. Dans le cas des courbes elliptiques définies sur les corps de fonctions, on sait depuis les travaux de Deligne, Drinfeld et Zarhin qu'une courbe elliptique est modulaire si elle possède une mauvaise réduction multiplicative totalement décomposée en la place ∞.
La construction de la paramétrisation modulaire due à Gekeler et Reversat est plus complexe et fait appel à de nombreux outils théoriques. Notre travail aboutit sur une formule explicite pour le calcul des images des pointes par la paramétrisation modulaire, et sur un résultat permettant de donner une borne sur l'ordre de ces images.

Dans la suite de ce chapitre, nous faisons des rappels sur les courbes elliptiques définies sur $\mathbb{Q}, \mathbb{C}$ et sur des corps complets non archimédiens. Nous

ferons également des rappels dans le monde "Drinfeld" sur de l'analyse non archimédienne, sur les modules de Drinfeld et sur la courbe modulaire de Drinfeld.

Courbes elliptiques

Définitions générales

Une courbe elliptique définie sur un corps k est une cubique qui peut se ramener par changement de variables à une cubique de Weierstrass non singulière. En d'autres termes, c'est une courbe projective sur $\mathbb{P}^2(k)$ donnée par une équation de la forme

$$E\colon Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in k,$$

ne possédant pas de point singulier. Ici le point $O = [0, 1, 0]$ est le point de base. Il est invariant par les changements de variables dits *admissibles* qui sont de la forme

$$\begin{aligned} X &= u^2X' + r, \\ Y &= u^3Y' + sX' + t, \end{aligned}$$

avec $u \in k^*$ et $r, s, t \in k$. Les autres points projectifs $P = [x_0, y_0, z_0]$ de E vérifient $z_0 \neq 0$ et donc peuvent s'écrire sous la forme $P = [x_0/z_0, y_0/z_0, 1]$. De tels points s'identifient naturellement aux points du modèle affine

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

Par abus, on donnera toujours une courbe elliptique par une équation de Weierstrass affine et notera l'ensemble des points k-rationnels

$$E(k) = \{(x, y) \in k^2,\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

On considère la quantité Δ appelée le discriminant de E qui est un polynôme en les coefficients a_1, a_2, a_3, a_4 et a_6 (voir [42, chapitre 3]). La condition de non-singularité est équivalente à $\Delta \neq 0$. On considère la quantité j appelée le j-invariant de E qui est une fraction rationnelle en les coefficients a_i, $i \in \{1, 2, 3, 4, 6\}$ (voir [42, chapitre 3]). Cette quantité est invariante par les changements de variables admissibles.

Une courbe elliptique E définie sur un corps k peut être munie d'une loi de groupe abélien. Considérons P, Q deux points de $E(k)$. La droite $\mathcal{L} \subset \mathbb{P}^2(k)$ reliant P à Q coupe une troisième fois la courbe E par le théorème de Bézout [28, Théorème A.4.6.1] en un point R. On définit le point $P+Q \in E(k)$

comme le troisième point d'intersection entre la droite $\mathcal{L}' \subset \mathbb{P}^2(k)$ reliant R au point infini O et la courbe E. L'ensemble $E(k)$ muni de la loi $+$ est un groupe abélien dont l'élément neutre est le point O.

Soient E, E' deux courbes elliptiques définies sur un corps k. Une isogénie est un morphisme de courbes

$$\phi\colon E \to E',$$

satisfaisant $\phi(O) = O$. Deux courbes elliptiques sont dites isogènes s'il existe une isogénie ϕ telle que $\phi(E) \neq \{O\}$. Une isogénie $\phi\colon E \to E'$ donne un morphisme de groupes $E(k) \to E'(k)$. En particulier si k est algébriquement clos et $\phi(E) \neq \{O\}$, alors $\phi(E(k)) = E'(k)$.

Courbes elliptiques définies sur $\mathbb{C}$

Les courbes elliptiques définies sur $\mathbb{C}$ peuvent être également définies de manière analytique. On considère $\Lambda \subset \mathbb{C}$ un $\mathbb{Z}$-réseau de rang 2 (c'est-à-dire un $\mathbb{Z}$-module discret de rang 2). Le réseau Λ peut se ramener par une homothétie à un réseau de la forme $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ avec $\omega_1, \omega_2 \in \mathbb{C}$ qui vérifient $\mathrm{Im}\left(\dfrac{\omega_2}{\omega_1}\right) > 0$. On définit la fonction de Weierstrass $\wp_\Lambda$ associée à Λ par

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

La fonction ainsi définie est une fonction elliptique, c'est-à-dire une fonction méromorphe doublement périodique. Cette fonction satisfait l'équation fonctionnelle suivante

$$\left(\frac{1}{2}\wp'_\Lambda(z)\right)^2 = \wp^3_\Lambda(z) - g_2\wp_\Lambda(z) - g_3,$$

où $g_2 = g_2(\Lambda) = 15{\sum_{\omega\in\Lambda}}' \dfrac{1}{\omega^4}$, et $g_3 = g_3(\Lambda) = 35{\sum_{\omega\in\Lambda}}' \dfrac{1}{\omega^6}$. On a le morphisme de groupes analytiques suivant

$$\begin{array}{rccl} \wp\colon & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) \\ & z \mod \Lambda & \mapsto & \begin{cases} (\wp_\Lambda(z), \frac{1}{2}\wp'_\Lambda(z)) & \text{si} \quad z \notin \Lambda, \\ O & \text{si} \quad z \in \Lambda. \end{cases} \end{array}$$

où E est la courbe elliptique définie sur $\mathbb{C}$ par l'équation $y^2 = x^3 - g_2x - g_3$.

Théorème 1. *(Uniformisation de Tate [42])*
Soient $A, B \in \mathbb{C}$ tels que $A^3 - 27B^2 \neq 0$. Alors il existe un réseau unique à homothétie près $\Lambda \subset \mathbb{C}$ tel que $g_2(\Lambda) = A$ et $g_3(\Lambda) = B$.

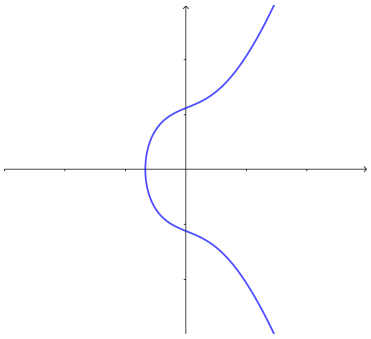
La conséquence directe du théorème d'uniformisation de Tate est que si E est une courbe elliptique définie sur $\mathbb{C}$, alors il existe un unique réseau à homothétie près $\Lambda \subset \mathbb{C}$ et un isomorphisme analytique $\wp\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$.

Si l'on regarde les courbes elliptiques définies sur $\mathbb{R}$, on a la propriété suivante :

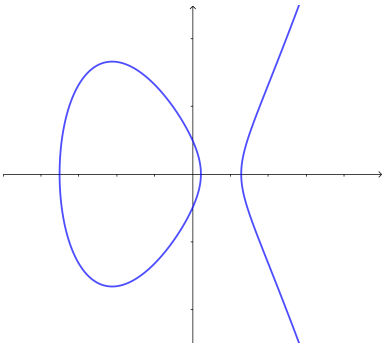
Proposition 2. *[45, Chapitre V, Corollaire 2.3.1] Soit E une courbe elliptique définie sur $\mathbb{R}$ de discriminant Δ. Alors on a*

$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{si} \quad \Delta < 0, \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si} \quad \Delta > 0. \end{cases}$$

En particulier, lorsqu'une courbe elliptique E est définie sur $\mathbb{R}$, il y a deux possibilités pour $E(\mathbb{R})$: soit $E(\mathbb{R})$ possède une unique composante connexe (lorsque $\Delta < 0$), soit $E(\mathbb{R})$ possède deux composantes connexes (lorsque $\Delta > 0$).



$y^2 = x^3 + ax + b$
avec $\Delta < 0$



$y^2 = x^3 + ax + b$
avec $\Delta > 0$

Courbes elliptiques définies sur $\mathbb{Q}$

L'étude des points rationnels d'une courbe elliptique définie sur $\mathbb{Q}$ trouve ses premières motivations dans la résolution d'équations diophantiennes. Un résultat bien connu des courbes elliptiques définies sur $\mathbb{Q}$ est le théorème de Mordell-Weil :

Théorème 3. *[42, Théorème 6.7] Soit E une courbe elliptique définie sur $\mathbb{Q}$ alors le groupe abélien $(E(\mathbb{Q}),+)$ est de type fini. En d'autres termes il existe un entier $r \geq 0$ tel que*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}},$$

où $E(\mathbb{Q})_{\text{tors}} = \{P \in E(\mathbb{Q}), \text{il existe } m \in \mathbb{N}^*, mP = O\}$ est fini.

L'entier r du théorème est appelé le rang de $E(\mathbb{Q})$. Ce théorème reste vrai lorsque l'on remplace $\mathbb{Q}$ par un corps de nombres. Le groupe de torsion de E est facile à calculer et pour une courbe elliptique E définie sur $\mathbb{Q}$ il y a un nombre fini de groupes de torsion possibles. En effet, on a par un résultat de Mazur ([31]) : $\#E(\mathbb{Q})_{\text{tors}} \leq 16$.

La notion de hauteur désigne la mesure de la complexité algébrique d'une solution d'une équation diophantienne. La théorie des hauteurs joue un rôle important en arithmétique diophantienne dans la démonstration du théorème de Mordell-Weil. Il est possible de définir la hauteur sur une courbe elliptique définie sur un corps de nombres. On se contentera de la définition de la hauteur pour des courbes elliptiques définies sur $\mathbb{Q}$. Soit $E/\mathbb{Q}$ une courbe elliptique donnée par un modèle de Weierstrass et $P = (x, y) \in E(\mathbb{Q})$ avec $x = \frac{r}{s}$ vérifiant $\text{pgcd}(r, s) = 1$. On définit la hauteur naïve de P comme $h(P) = \log \max(|r|, |s|)$, et par convention on pose $h(O) = 0$. La hauteur canonique est l'application $\widehat{h}$: $E(\mathbb{Q}) \to \mathbb{R}$, définie par

$$\widehat{h}(P) = \frac{1}{2} \lim_{k \to \infty} \frac{h(2^k P)}{2^{2k}}.$$

À noter que l'application $\widehat{h} - \frac{1}{2}h$ est bornée sur E. L'application $\widehat{h}$ satisfait les relations suivantes :

Proposition 4. *Soit E une courbe elliptique définie sur $\mathbb{Q}$. On a :*

1. *Pour tous $P, Q \in E(\mathbb{Q})$, $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$.*
2. *Pour tout $P \in E(\mathbb{Q})$, $\widehat{h}(P) = 0$ si et seulement si $P \in E(\mathbb{Q})_{\text{tors}}$.*
3. *Pour tout $P \in E(\mathbb{Q})$ et pour tout $k \in \mathbb{Z}$, $\widehat{h}(kP) = k^2\widehat{h}(P)$.*

La hauteur canonique jouera un rôle clé dans la démonstration du théorème principal du chapitre 1.

Courbes elliptiques définies sur $\mathbb{Q}(T)$

Si E est une courbe elliptique définie sur $\mathbb{Q}(T)$, alors pour tout $t \in \mathbb{Q}$, on note $E(t)$ la spécialisation de E en $T = t$. À noter que $E(t)$ est une courbe elliptique pour tous sauf un nombre fini de $t \in \mathbb{Q}$. On rappelle qu'il existe des morphismes de spécialisation notés σ_t :

$$\sigma_t \colon E(\mathbb{Q}(T)) \to E(t)(\mathbb{Q}).$$

Néron a montré dans [33] que les applications $(\sigma_t)_{t\in\mathbb{Q}}$ sont injectives pour tous sauf un nombre fini de $t \in \mathbb{P}^1(\mathbb{Q})$. La définition suivante est le cadre du travail réalisé dans le chapitre 1.

Définition 5. *Soit E une courbe elliptique définie sur $\mathbb{Q}(T)$, et soit $t \in \mathbb{Q}$. On dit que $\sigma_t(E(\mathbb{Q}(T)))$ est divisible s'il existe $P \in E(t)(\mathbb{Q})$, $n \geq 2$ tel que $nP \in \sigma_t(E(\mathbb{Q}(T)))$ et $P \notin \sigma_t(E(\mathbb{Q}(T)))$. Dans le cas contraire, on dit que $\sigma_t(E(\mathbb{Q}(T)))$ est non divisible.*

On rappelle que si $A \subset \mathbb{N}$ est une partie infinie de $\mathbb{N}$, la densité naturelle de A est définie comme

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \in A,\ n \leq N\}, \text{ si la limite existe.}$$

On rappelle également qu'une courbe elliptique E définie sur $\mathbb{Q}(T)$ est dite isotriviale si le j-invariant de E est constant. On a le théorème de spécialisation suivant établi par Silverman dans [41].

Théorème 6. *Soit E une courbe elliptique définie sur $\mathbb{Q}(T)$ non isotriviale. L'ensemble des $t \in \mathbb{N}^*$ tels que $\sigma_t(E(\mathbb{Q}(T)))$ est non divisible est de densité naturelle* 1.

Courbes elliptiques définies sur un corps complet non archimédien

Lorsque que E est définie sur un corps complet K non-archimédien, l'uniformisation de Tate par un réseau additif n'est pas possible. Néanmoins, Tate introduit une uniformisation multiplicative dans [46] que nous allons rappeler brièvement. Soit K un corps complet pour une norme $|\cdot|_v$. Soit $t \in K^*$ tel que $|t|_v < 1$. On pose les quantités

$$a_4(t) = 5\sum_{n=1}^{\infty} \frac{n^3 t^n}{1-t^n}, \qquad a_6(t) = \sum_{n=1}^{\infty} \frac{7n^5+5n^3}{12} \frac{t^n}{1-t^n}. \tag{2}$$

On remarque que $7n^5+5n^3 \equiv 0[12]$ et que par conséquent le coefficient $a_6(t)$ a bien un sens même en caractéristique 2 et 3. On définit la courbe de Tate E_t par l'équation

$$E_t\colon y^2+xy = x^3+a_4(t)x+a_6(t).$$

Les séries suivantes :

$$X(u,t) = \sum_{n\in\mathbb{Z}} \frac{t^n u}{(1-t^n u)^2} - 2\sum_{n\geq 1}\frac{nt^n}{1-t^n},$$
$$Y(u,t) = \sum_{n\in\mathbb{Z}} \frac{(t^n u)^2}{(1-t^n u)^3} + \sum_{n\geq 1}\frac{nt^n}{1-t^n},$$

convergent pour tout $u \in K^* - t^{\mathbb{Z}}$. Elles définissent un morphisme surjectif

$$\begin{array}{rccl} \phi\colon & \overline{K} & \to & E_t(\overline{K}) \\ & u & \mapsto & \begin{cases} (X(u,t),Y(u,t)) & \text{si } u \notin t^{\mathbb{Z}}, \\ O & \text{sinon;} \end{cases} \end{array}$$

de noyau égal à $t^{\mathbb{Z}}$.

Théorème 7. *Soit K un corps complet pour une valuation discrète v.*

1. *Pour tout $t \in K^*$ vérifiant $|t|_v < 1$, l'application $\phi\colon \overline{K}/t^{\mathbb{Z}} \to E_t(\overline{K})$ est un isomorphisme de groupes.*
2. *Pour tout $j_0 \in K^*$, il existe $t \in K^*$ vérifiant $|t|_v < 1$ tel que E_t/K est une courbe elliptique caractérisée par $j(E_t) = j_0$ et E_t est de mauvaise réduction multiplicative déployée en v.*
3. *Soit E/K une courbe elliptique de j-invariant $j \in K$ vérifiant $|j|_v > 1$ et de réduction multiplicative déployée en v. Alors il existe $t \in K^*$ tel que E est isomorphe à E_t sur $\overline{K}$.*

Cadre général sur les corps de fonctions et modules de Drinfeld

Notations et préliminaires

Soit p un nombre premier et q une puissance de p. On note $K = \mathbb{F}_q(T)$ et $A = \mathbb{F}_q[T]$. Le corps $K_\infty = \mathbb{F}_q((\frac{1}{T}))$ est un complété de K pour la norme $|P| = q^{\deg(P)}$ associée à la valuation $v_\infty(P) = -\deg(P)$. Soit $\pi = 1/T$ qui

est une uniformisante de K_∞. On définit $O_\infty = \{x \in K_\infty, |x| \leq 1\} = \mathbb{F}_q[[\pi]]$ l'anneau des entiers π-adiques. Soit $\overline{K_\infty}$ une clôture algébrique de K_∞. On fixe $\mathbb{C}_\infty$ un complété de $\overline{K_\infty}$.
Un sous-groupe de $\mathrm{Gl}_2(A)$ est dit de congruence (ou sous-groupe arithmétique) s'il contient un sous-groupe de la forme

$$\Gamma(n) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(A),\ \gamma \equiv I_2[n] \right\},$$

avec $n \in A$ unitaire non constant. Le sous-groupe

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(A), c \equiv 0[n] \right\}$$

en est un exemple.

Soit $\Omega = \mathbb{C}_\infty - K_\infty$ le demi-plan de Drinfeld. Sur $\mathbb{C}_\infty$ la "partie imaginaire" notée $|.|_i$ est définie par $|z|_i = \inf\{|z - x|,\ x \in K_\infty\}$. Le groupe $\mathrm{Gl}_2(K_\infty)$ agit par homographies sur Ω, c'est-à-dire par

$$\gamma z = \frac{az + b}{cz + d} \qquad \text{où } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(K_\infty) \text{ et } \ z \in \Omega.$$

Proposition 8. *[26] Soit $z \in \mathbb{C}_\infty$. On a les propriétés suivantes :*

1. *On a $|z|_i = 0$ si et seulement si $z \in K_\infty$.*
2. *Pour tout $x \in K_\infty$, $|xz|_i = |x||z|_i$.*
3. *Si $|z| \notin q^{\mathbb{Z}}$ alors $|z|_i = |z|$.*
4. *Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(K_\infty)$, alors $|\gamma z|_i = \dfrac{|\det(\gamma)|}{|cz + d|^2} |z|_i$.*

Analyse non archimédienne

On rappelle que $\mathbb{C}_\infty$ est un corps complet algébriquement clos pour une norme ultramétrique. La proposition suivante existe très certainement dans la littérature mais comme nous ne l'avons pas trouvée, nous en donnons une démonstration. Cette proposition sera utile dans le chapitre 2, notamment pour la définition des fonctions thêta.

Proposition 9. *Soit K un corps complet pour une norme $|\cdot|$ ultramétrique. Soit $(a_n)_{n\in\mathbb{N}} \subset K$ tel que $\sum_{n\in\mathbb{N}} a_n$ (respectivement $\prod_{n\in\mathbb{N}} a_n$) converge. Alors la série $(\sum_{n\in\mathbb{N}} a_n)$ (respectivement le produit $\prod_{n\in\mathbb{N}} a_n$) ne dépend pas de l'ordre de sommation (respectivement l'ordre du produit).*

Démonstration. On ne démontre le résultat que dans le cas des sommes. Dans le cas des produits la preuve utilise des arguments similaires.
Soit $(a_n)_{n\in\mathbb{N}} \subset K$ une suite telle que $(\sum_{n\geq 0} a_n)$ converge. Il existe donc $a \in K$ tel que

$$\sum_{n=0}^{N} a_n \underset{N\to\infty}{\to} a.$$

On considère $\varphi\colon \mathbb{N} \to \mathbb{N}$ une bijection. On va montrer que $(\sum_{n\geq 0} a_{\varphi(n)})$ converge également vers a. Fixons $\varepsilon > 0$. On sait qu'il existe $n_0 \geq 0$ tel que pour tout $N \geq n_0$, $|a_N| \leq \varepsilon$. À noter que comme la norme est ultramétrique, on a pour tout $N \geq n_0$, $|\sum_{n\leq N} a_n - a| \leq \varepsilon$. D'autre part, comme φ est une bijection, il existe $n_1 \geq 0$ tel que pour tout $n \geq n_1$, $\varphi(n) \geq n_0$. Soit $N \geq \max(n_1, n_0)$. Alors

$$\left|\sum_{n=0}^{N} a_{\varphi(n)} - a\right| \leq \underbrace{\left|\sum_{n=0}^{N} a_n - a\right|}_{\leq\varepsilon} + \left|\sum_{n=0}^{N} a_n - \sum_{n=0}^{N} a_{\varphi(n)}\right|.$$

On a

$$\begin{aligned}\sum_{n\leq N} a_n = \sum_{n\leq n_0} a_n + \sum_{n_0<n\leq N} a_n &= \sum_{\substack{k\in\mathbb{N}\\ \varphi(k)<n_0}} a_{\varphi(k)} + \sum_{n_0<n\leq N} a_n \\ &= \sum_{\substack{k<n_1\\ \varphi(k)<n_0}} a_{\varphi(k)} + \sum_{n_0<n\leq N} a_n\end{aligned}$$

Il vient

$$\begin{aligned}\left|\sum_{n=0}^{N} a_n - \sum_{n=0}^{N} a_{\varphi(n)}\right| &= \left|\sum_{n_0<n\leq N} a_n - \sum_{\substack{n\leq N\\ \varphi(n)\geq n_0}} a_{\varphi(n)}\right| \\ &\leq \max\left(\left|\sum_{n_0<n\leq N} a_n\right|, \left|\sum_{\substack{n\leq N\\ \varphi(n)\geq n_0}} a_{\varphi(n)}\right|\right) \\ &\leq \varepsilon.\end{aligned}$$

D'où

$$\left|\sum_{n=0}^{N} a_{\varphi(n)} - a\right| \leq 2\varepsilon.$$

□

Pour $a \in \mathbb{C}_\infty$, et $r > 0$. Un réel positif, on note $D(a, r)$ le disque

$$\{z \in \mathbb{C}_\infty, |z - a| < r\}.$$

Définition 10. *Soient $a \in \mathbb{C}_\infty$ et $r > 0$. Une fonction $f\colon D(a, r) \to \mathbb{C}_\infty$ est dite holomorphe (ou analytique) s'il existe une série entière $\sum_{n\geq 0} a_n X^n$ telle que $f(z) = \sum_{n\geq 0} a_n (z - a)^n$ pour tout $z \in D(a, r)$.*
Soit $U \subset \mathbb{C}_\infty$ un ouvert, une fonction $f\colon U \to \mathbb{C}_\infty$ est dite holomorphe (ou analytique) si pour tout $a \in U$ et tout $r \in \mathbb{R}_+^*$, f est analytique sur $D(a, r) \cap U$.
Une fonction $f\colon U \to \mathbb{C}_\infty$ est dite méromorphe s'il existe une fonction holomorphe non nulle $g\colon U \to \mathbb{C}_\infty$ ne possédant pas de pôles telle que fg est une fonction holomorphe sur U.

À noter que la propriété "f est holomorphe sur U" est équivalente à "f est limite uniforme de fonction rationnelle sans pôles sur U".

Modules de Drinfeld

Les modules de Drinfeld seront définis[1] sur $A = \mathbb{F}_q[T]$.

Définition 11. *Soit L un corps. On dit que L est un A-corps s'il existe un morphisme de $\mathbb{F}_q$-algèbres $\delta\colon A \to L$. On dit que $\mathrm{Ker}(\delta)$ est la A-caractéristique de L.*

Nous nous restreignons au cas où la A-caractéristique de L est 0. On considère $\tau\colon x \mapsto x^q$ l'endomorphisme de Frobenius. On note $L\{\tau\}$ l'algèbre engendrée par τ sur L. Rappelons que cette algèbre est non commutative. En effet, on a :

$$\tau\ell = \ell^q\tau, \qquad (\ell \in L).$$

Pour $P = \sum_{i=0}^n c_i\tau^i \in L\{\tau\}$, on pose $D(P) = c_0$.

Définition 12. *Soit L un corps. Un module de Drinfeld est la donnée d'un morphisme de $\mathbb{F}_q$-algèbres $\delta\colon A \to L$ et d'un morphisme de $\mathbb{F}_q$-algèbres $\phi\colon A \to L\{\tau\}$ satisfaisant :*

1. *il existe $a \in A$, $\phi(a) \notin L$;*
2. *pour tout $a \in A$, $D(\phi(a)) = \delta(a)$.*

L'image de $a \in A$ par un module de Drinfeld ϕ est notée ϕ_a.

1. Il est possible définir les modules de Drinfeld à partir de n'importe quel anneau des fonctions régulières d'un corps de fonctions d'une courbe définie sur $\mathbb{F}_q$.

Proposition 13. *Soit ϕ un A-module de Drinfeld sur L. Il existe un entier $r \geq 1$ tel que pour tout $a \in A, \deg_\tau(\phi_a) = r\deg(a)$. Cet entier est appelé le rang de ϕ.*

Définition 14. *Soient ϕ, ϕ' deux A-modules de Drinfeld sur un A-corps L. Un morphisme de ϕ dans ϕ' est un élément $f \in L\{\tau\}$ vérifiant $f\phi_a = \phi'_a f$, pour tout $a \in A$. On note $\mathrm{Hom}_A(\phi, \phi')$ l'ensemble des morphismes de ϕ dans ϕ'. On dit que ϕ et ϕ' sont isogènes si $\mathrm{Hom}_A(\phi, \phi') \neq \{0\}$.*

À noter que deux modules de Drinfeld isogènes sont toujours de même rang.

Définition 15. *Soient ϕ, ϕ' deux A-modules de Drinfeld sur un A-corps L et $f \in L\{\tau\}$ un morphisme de ϕ dans ϕ'. On dit que f est isomorphisme s'il existe un morphisme g de ϕ dans ϕ' tel que $fg = \tau^0 = gf$. Deux modules de Drinfeld sont dit isomorphes s'il existe un isomorphisme entre les deux.*

Il existe également une uniformisation pour les modules de Drinfeld définis sur $\mathbb{C}_\infty$, par les A-réseaux de $\mathbb{C}_\infty$. Un A-réseau de $\mathbb{C}_\infty$ est un A-module discret de type fini. On appelle rang d'un A-réseau son rang en tant que A-module libre. En conséquence si Λ est un A-réseau de $\mathbb{C}_\infty$ de A-base $(\omega_1, ..., \omega_r) \in \mathbb{C}_\infty^r$, alors $\omega_1, ..., \omega_r$ sont K_∞-linéairement indépendants. Soit Λ, Λ' deux A-réseaux de $\mathbb{C}_\infty$. On note

$$\mathrm{Hom}(\Lambda, \Lambda') = \{c \in \mathbb{C}_\infty,\ c\Lambda \subset \Lambda'\}.$$

On dit que Λ et Λ' sont homothétiques si $\mathrm{Hom}(\Lambda, \Lambda') \neq \{0\}$ et que Λ, Λ' sont isomorphes s'il existe $c \in \mathbb{C}_\infty^*$ tel que $c\Lambda = \Lambda'$.
Soit $\Lambda \subset \mathbb{C}_\infty$ un A-réseau. On considère la fonction

$$\begin{array}{rccc} e_\Lambda : & \mathbb{C}_\infty & \to & \mathbb{C}_\infty \\ & z & \mapsto & z \displaystyle\prod_{\lambda \in \Lambda - \{0\}} \left(1 - \frac{z}{\lambda}\right), \qquad z \in \mathbb{C}_\infty. \end{array}$$

Cette fonction est appelée l'exponentielle de Carlitz associée à Λ. Elle est $\mathbb{F}_q$-linéaire, surjective et de noyau égal à Λ. On pose également :

$$P_a^\Lambda(z) = z \prod_{\lambda \in a^{-1}\Lambda/\Lambda - \{0\}} \left(1 - \frac{z}{e_\Lambda(\lambda)}\right), \qquad a \in A, \quad z \in \mathbb{C}_\infty.$$

Puisque la fonction e_Λ est Λ-périodique, le produit définissant P_a^Λ est indépendant du système de représentants choisi pour $a^{-1}\Lambda/\Lambda$ et donc P_a^Λ est bien défini.

Théorème 16. *Soit $\Lambda \subset \mathbb{C}_\infty$, un A-réseau de rang r. Pour tout $a \in A$, et $z \in \mathbb{C}_\infty$, on définit $\Phi_a^\Lambda(z) = aP_a^\Lambda(z)$. Alors l'application $a \in A \mapsto \phi_a^\Lambda \in \mathbb{C}_\infty\{\tau\}$ est un module de Drinfeld sur $\mathbb{C}_\infty$ de rang r.*

Soit $\Lambda \subset \mathbb{C}_\infty$ un A-réseau et ϕ^Λ le module de Drinfeld associé. On a l'équation fonctionnelle suivante :

$$\phi_a^\Lambda(e_\Lambda(z)) = e_\Lambda(az), \qquad a \in A, \quad z \in \mathbb{C}_\infty.$$

Théorème 17. *[27, Théorème 4.6.9] Soit ϕ un module de Drinfeld défini sur $\mathbb{C}_\infty$ de rang $r \geq 1$, alors il existe un A-réseau de rang r de $\mathbb{C}_\infty$ unique à isomorphisme près Λ tel que $\phi^\Lambda = \phi$.*

Une des conséquences de ce théorème est que l'on peut caractériser la notion d'isogénie entre modules de Drinfeld sur $\mathbb{C}_\infty$ de la manière suivante :

Proposition 18. *[27] Soient ϕ, ϕ' deux modules de Drinfeld sur $\mathbb{C}_\infty$ de réseaux associés respectifs Λ, Λ'. Alors ϕ et ϕ' sont isogènes si et seulement si Λ et Λ' sont homothétiques.*

Théorème 19. *Soient $\Lambda, \Lambda' \in \mathbb{C}_\infty$ deux réseaux homothétiques. Soit $c \in \mathrm{Hom}(\Lambda, \Lambda')$ une homothétie non nulle. On définit*

$$f_c(z) = cP_{c^{-1}}(z), \quad z \in \mathbb{C}_\infty.$$

Alors $f_c \in \mathrm{Hom}_A(\phi^\Lambda, \phi^{\Lambda'})$. De plus, l'application $c \mapsto f_c$ définit un isomorphisme de $\mathrm{Hom}(\Lambda, \Lambda')$ dans $\mathrm{Hom}_A(\phi^\Lambda, \phi^{\Lambda'})$.

Définition 20. *Soient ϕ, ϕ' deux modules de Drinfeld isogènes sur $\mathbb{C}_\infty$, de rang r et de réseaux associés Λ, Λ'. Soient $f \in \mathrm{Hom}_A(\phi, \phi')$ une isogénie et $c \in \mathbb{C}_\infty$ tel que $f(z) = cP_{c^{-1}}(z)$. On appelle degré de f l'unique élément $n \in A$ unitaire tel que*

$$c^{-1}\Lambda'/\Lambda \simeq (A/n)^r .$$

Les modules de Drinfeld de rang 2 sur $\mathbb{C}_\infty$ présentent certaines analogies avec les courbes elliptiques définies sur $\mathbb{C}$. Soit ϕ un module de Drinfeld de rang 2 sur $\mathbb{C}_\infty$. Alors ϕ est caractérisé par

$$\phi_T = T + g\tau + \Delta\tau^2,$$

avec $g, \Delta \in \mathbb{C}_\infty$, $\Delta \neq 0$. On pose $j(\phi) = \dfrac{g^{q+1}}{\Delta}$. Si ϕ et ϕ' sont deux modules de Drinfeld sur $\mathbb{C}_\infty$ de rang 2 alors ϕ et ϕ' sont isomorphes sur $\mathbb{C}_\infty$ si et seulement si $j(\phi) = j(\phi')$. Si ϕ est un module de Drinfeld sur $\mathbb{C}_\infty$, par le théorème d'uniformisation de Tate-Drinfeld il existe un A-réseau de rang 2 de la forme $\Lambda = A\omega_1 + A\omega_2 \subset \mathbb{C}_\infty$ tel que $\phi = \phi^\Lambda$. Ici $\omega_1, \omega_2 \in \mathbb{C}_\infty$ sont K_∞-linéairement indépendants. On peut prendre $\omega_1 = 1$ et $\omega_2 = z \in \Omega$.

Courbe modulaire de Drinfeld

Soit $n \in A$ un polynôme unitaire non constant. D'un point de vue géométrique, la courbe modulaire $\mathcal{X}_0(n)$ qui est une courbe projective lisse sur K est la compactification de la courbe algébrique $\mathcal{Y}_0(n)$ (voir [15]), cette dernière classifie à isomorphisme près les couples de modules de Drinfeld (ψ_1, ψ_2) définis sur $\mathbb{C}_\infty$ de rang 2 munis d'une isogénie $\rho\colon \psi_1 \to \psi_2$ de degré n. De manière analytique, on sait par le théorème d'uniformisation de Tate-Drinfeld qu'à tout module de Drinfeld de rang 2 correspond un A-réseau de rang 2 unique à homothétie près. On peut considérer que le couple (ψ_1, ψ_2) comme un couple de la forme

$$((A + Az), (A + Anz)),$$

avec $z \in \Omega$. Deux points z et z' représentent le même point sur la courbe modulaire si et seulement s'il existe $\gamma \in \Gamma_0(n)$ telle que $\gamma z = z'$. On note $\overline{\Omega} := \Omega \cup \mathbb{P}^1(K)$. L'action de $\mathrm{Gl}_2(A)$ sur Ω se prolonge à $\overline{\Omega}$ de la manière suivante :

$$\gamma z = \begin{cases} \dfrac{az+b}{cz+d} & \text{si } z \in \Omega, \\ [au+bv, cu+vd] & \text{si } z = [u,v] \in \mathbb{P}^1(K). \end{cases}$$

Le sous-groupe $\Gamma_0(n)$ agissant sur Ω avec un nombre fini de stabilisateurs il vient que $M_{\Gamma_0(n)} := \Gamma_0(n)\backslash\Omega$ peut être muni d'une structure d'espace analytique sur K_∞. On a un isomorphisme d'espace analytique $M_{\Gamma_0(n)}(\mathbb{C}_\infty) \simeq \mathcal{Y}_0(n)(\mathbb{C}_\infty)$. L'espace $\overline{M}_{\Gamma_0(n)} = \Gamma_0(n)\backslash\overline{\Omega}$ est la version analytique de la courbe modulaire $\mathcal{X}_0(n)$ (voir [18, chapitre V]). Les pointes de $\overline{M}_{\Gamma_0(n)}$ sont les orbites de $K \cup \{\infty\}$ par l'action de $\Gamma_0(n)$. Elles sont en bijection avec l'ensemble $\Gamma_0(n)\backslash\mathbb{P}^1(K)$. Par conséquent les pointes de la courbe modulaire $M_{\Gamma_0(n)}$ sont en nombre fini.

Plan de la thèse

Dans cette thèse, on étudie à travers deux chapitres indépendants deux aspects explicite différents des courbes elliptiques dans deux contextes différents.

Dans le premier chapitre on étudie la question de la non-divisibilité d'un point sur une famille de courbes elliptiques à deux paramètres définies sur $\mathbb{Q}$. La famille qui nous intéresse est donnée par l'équation

$$\mathcal{E}_n\colon y^2 = x^3 + Tx^2 - n^2(T + 3n^2)x + n^6,$$

avec n un entier strictement positif. Cette famille est un cas spécial ($a = \pm n^2$) de la famille étudiée par Bettin, David, Delaunay dans [3]. Il s'agit des valeurs de $a \in \mathbb{Q}^*$ où la courbe elliptique est de rang 1 sur $\mathbb{Q}(T)$. Cette famille possède le point $(0, n^3)$ comme point d'ordre infini. Notre attention s'est portée sur les spécialisations de T en des entiers non nuls t tels que le point $(0, n^3)$ est non divisible. Pour le cas $n = 1$, et $t > 0$, un résultat de Duquesne dans [16] assure que si $t^2 + 3t + 9$ est sans facteurs carrés alors le point $(0, 1)$ est non divisible. Le résultat principal qui le généralise assure que le point $(0, n^3)$ est non divisible lorsque t est suffisamment grand comparé à n et que la quantité $t^2 + 3n^2t + 9n^4$ est sans facteurs carrés. Pour ce faire nous utiliserons des propriétés de la hauteur canonique sur les courbes elliptiques, des méthodes de calcul approché des périodes de ces courbes, ainsi que des propriétés arithmétiques vérifiées par la famille.

Dans le second chapitre, nous nous intéressons à la paramétrisation modulaire sur les corps de fonctions. La situation est la suivante : si E est une courbe elliptique non-isotriviale définie sur $\mathbb{F}_q(T)$ de mauvaise réduction multiplicative déployée en la place $\infty := 1/T$, alors il existe un paramètre $t \in \mathbb{C}_\infty^*$ tel que $E(\mathbb{C}_\infty) \simeq \mathbb{C}_\infty^*/t^{\mathbb{Z}}$, où $\mathbb{C}_\infty$ est le complété d'une clôture algébrique de $\mathbb{F}_q\left(\left(\frac{1}{T}\right)\right)$. D'après les travaux de Grothendieck, Jacquet et Langlands, et Drinfeld dans les années soixante-dix, il existe une application rationnelle $\Phi\colon \mathcal{X}_0(n) \to E$, où n est le conducteur de E et $\mathcal{X}_0(n)$ est la courbe modulaire de Drinfeld. Une description concrète de cette application est possible et l'image d'un point de la courbe modulaire peut être calculée explicitement grâce aux travaux de Gekeler et Reversat [26]. Le résultat principal de ce chapitre est une formule permettant de calculer explicitement l'image d'une pointe par la paramétrisation modulaire. Un résultat analogue au théorème de Manin-Drinfeld, montré par Gekeler, assure que l'image d'une pointe de $\overline{M}_{\Gamma_0(n)}$ est un point de torsion sans pour autant donner une borne sur l'ordre de ce point. Ce résultat sera redémontré avec une preuve alternative qui permet d'obtenir une borne sur l'ordre de ces points. Pour cette étude, on a besoin d'introduire des outils théoriques qui jouent un rôle important dans la construction de la paramétrisation modulaire. Ces résultats sont illustrés avec des exemples sur $\mathbb{F}_2$ et $\mathbb{F}_3$ de courbes elliptiques de conducteurs de petits degrés.

Finalement, en annexe on présente les programmes PARI/GP utilisés pour faire les calculs explicites dans les deux chapitres.

Chapitre 1

Non-divisibilité d'un point sur une famille de courbes elliptiques à deux paramètres

L'objectif de ce chapitre est de montrer la non-divisibilité d'un point sur une famille à deux paramètres de courbes elliptiques définies sur $\mathbb{Q}$. Cette famille est une généralisation de la famille de Washington [50] qui est liée à des corps cubiques cycliques. Soit n un entier strictement positif. On considère la courbe elliptique définie sur $\mathbb{Q}(T)$ donnée par

$$\mathcal{E}_n \colon y^2 = x^3 + Tx^2 - n^2(T + 3n^2)x + n^6. \tag{1.1}$$

Il s'agit d'un cas particulier des surfaces elliptiques étudiées par Bettin, David et Delaunay [3]. Le cas $n = 1$ est précisément la famille de Washington étudiée par Washington [50] et Duquesne [16]. Dans [3] les auteurs ont obtenu une formule pour la moyenne des *root numbers* des courbes elliptiques qui sont les spécialisations de $\mathcal{E}_n$ en $T = t \in \mathbb{Q}$. On note $\mathcal{E}_n(t)$ cette spécialisation.
Une autre courbe elliptique définie sur $\mathbb{Q}(T)$ provenant de cette famille est la suivante :

$$\mathcal{F}_n : y^2 = x^3 + Tx^2 + n^2(T - 3n^2)x - n^6. \tag{1.2}$$

Les deux courbes $\mathcal{E}_n$ et $\mathcal{F}_n$ sont reliées. En effet, pour tout entier strictement positif n et tout entier t, les courbes $\mathcal{E}_n(t-3n^2)$ et $\mathcal{F}_n(t)$ sont isomorphes sur $\mathbb{Q}$. Nous nous concentrerons donc sur $\mathcal{E}_n$.

Soit $t \in \mathbb{Z}$. Le théorème 5.7 de Duquesne dans [16] assure que si $n = 1$, t est positif et $t^2 + 3t + 9$ est sans facteurs carrés, alors le point $(0, 1)$ n'est pas divisible sur $\mathcal{E}_1(t)(\mathbb{Q})$. On généralise ce théorème de la manière suivante pour le point $(0, n^3)$:

Théorème 21. *Soit n un entier strictement positif et $t \in \mathbb{Z}$. On suppose que $t \geq \max(100n^2, 2n^4)$ ou $t \leq \min(-100n^2, -2n^4)$, et que $t^2 + 3n^2t + 9n^4$ est sans facteurs carrés. Alors le point $(0, n^3)$ n'est pas divisible sur $\mathcal{E}_n(t)(\mathbb{Q})$.*

Ce résultat a été publié dans le journal *Research in Number Theory* en 2022 ([36]). À notre connaissance, il n'existe pas de résultats similaires pour d'autres familles de courbes elliptiques définies sur $\mathbb{Q}$ possédant deux paramètres.

Une des conséquences du théorème 21 est que le point $(0, n^3)$ peut être choisi pour faire partie d'un système de générateurs de $\mathcal{E}_n(t)(\mathbb{Q})$ lorsque t est suffisamment grand. D'autre part, lorsque le rang de $\mathcal{E}_n(t)$ vaut un, il est alors possible de calculer l'ordre analytique du groupe de Tate-Shafarevich en utilisant la conjecture de Birch et Swinnerton-Dyer de la même manière que dans [14]. En particulier, on remarque qu'à l'exception du cas $n = 1$, le *root number* n'est ni constant ni équidistribué, ce qui motive l'étude de ce type de famille ([3]). Par exemple pour $n = 2$, la moyenne du *root number* est $-\frac{1}{2}$, ce qui signifie que 75 % des spécialisations possèdent un rang impair sous la conjecture de parité.

Pour tout entier strictement positif n, la courbe elliptique $\mathcal{E}_n$ est de rang 1 sur $\mathbb{Q}(T)$ et le point $(0, n^3)$ est d'ordre infini sur $\mathcal{E}_n(\mathbb{Q}(T))$ ([3], théorème 1). Le théorème de spécialisation de Silverman pour les surfaces elliptiques dans [41] a la conséquence suivante. Puisque l'application de spécialisation $\sigma_t \colon \mathcal{E}_n \to \mathcal{E}_n(t)$ n'est pas injective pour seulement un nombre fini de $t \in \mathbb{P}^1(\mathbb{Q})$, le théorème 21 implique que le point $(0, n^3)$ est un générateur de $\mathcal{E}_n(\mathbb{Q}(T))$. Cette propriété peut être démontrée de manière géométrique. En ce qui concerne la non-divisibilité (voir [41]) de l'image de $\mathcal{E}_n$ par l'application de spécialisation, le théorème 2 dans [41] assure que l'ensemble des $t \in \mathbb{Z}$ tels que $\sigma_t(\mathcal{E}_n)$ n'est pas divisible est de densité un. Notre théorème tient sous l'hypothèse $t^2 + 3n^2t + 9n^4$ sans facteurs carrés ce qui représente un ensemble de $t \in \mathbb{Z}$ de densité inférieure à 1 : cela donne un résultat moins fort que le résultat prédit par le théorème 2 de [41] mais il reste complètement explicite. D'autre part, pour tout entier strictement positif n, il existe un contre-exemple à la non-divisibilité lorsque $t^2 + 3n^2t + 9n^4$ possède au moins un facteur carré. Si $t = 5n^2$, on a $(0, n^3) = 3(-4n^2, 7n^3)$ ce qui montre que l'hypothèse sans facteurs carrés ne peut être supprimée du théorème 21. Cependant, nous n'avons pas trouvé d'autres exemples où le point $(0, n^3)$ est le multiple d'un autre point.

La stratégie pour démontrer le théorème 21 est similaire à celle de Duquesne avec un traitement supplémentaire spécifique et soigneux des deux paramètres (on remarque également qu'une petite erreur semble s'être glissée dans la Section 5D de [16] durant les calculs des contributions locales de

la hauteur, qu'on peut corriger ici). Supposons qu'il existe un entier $k \geq 2$ et un point $P \in \mathcal{E}_n(t)(\mathbb{Q})$ tel que $kP = (0, n^3)$. L'idée principale est de minimiser un tel entier k. La stratégie consiste à déterminer une minoration de la hauteur canonique $\widehat{h}(P)$ de P et une majoration de $\widehat{h}((0, n^3))$ (section 1.3), afin d'obtenir une contradiction. Pour ce faire, nous décomposerons la hauteur en contributions locales (section 1.3) et nous approcherons les périodes de $\mathcal{E}_n(t)$ (section 1.2).

1.1 Généralités sur la famille

Soit n un entier strictement positif et t un entier non nul. On considère la courbe elliptique

$$E : y^2 = x^3 + tx^2 - n^2(t + 3n^2)x + n^6, \tag{1.3}$$

précédemment notée $\mathcal{E}_n(t)$. On pose $\delta = t^2 + 3n^2t + 9n^4$. Le discriminant, le j-invariant, et le coefficient c_4 de E sont donnés par

$$\begin{aligned} \Delta &= 16n^4\delta^2, \\ j &= \tfrac{256}{n^4}\delta, \\ c_4 &= 16\delta. \end{aligned}$$

Soit f le polynôme

$$f(x) = x^3 + tx^2 - n^2(t + 3n^2)x + n^6.$$

Le discriminant de f est $n^4\delta^2$, qui est positif, donc f possède trois racines réelles notées $\alpha_1 < \alpha_2 < \alpha_3$. Elles vérifient $\alpha_1 < 0 < \alpha_2 < n^2 < \alpha_3$. Le polynôme f est irréductible sur $\mathbb{Q}$ si δ est sans facteurs carrés. En effet, il suffit de remarquer que le polynôme $h(x) = 27f\left(\dfrac{x-t}{3}\right) = x^3 + 3\delta x + \delta(2t + 3n^2)$ est irréductible par le critère d'Eisenstein. Sans la condition que δ est sans facteurs carrés, l'irréductibilité de f sur $\mathbb{Q}$ semble être vraie pour une infinité de valeurs de t. On peut toutefois trouver des contre-exemples : par exemple pour $n = 2$ et $t = -6$, on a $f(x) = (x + 4)(x - 2)(x - 8)$.

On note $E_0(\mathbb{R})$ la composante connexe de l'identité et $E(\mathbb{R}) - E_0(\mathbb{R})$ la composante connexe bornée de $E(\mathbb{R})$. On rappelle que $E_0(\mathbb{R})$ est un sous-groupe $E(\mathbb{R})$ et que la somme de deux points de $E(\mathbb{R}) - E_0(\mathbb{R})$ appartient à $E_0(\mathbb{R})$. Le point entier $(0, n^3)$ appartient à $E(\mathbb{Q})$ pour tous entiers t et n. Plus précisément, le fait que $\alpha_2 > 0$ implique que $(0, n^3)$ appartient à $E(\mathbb{Q}) - E_0(\mathbb{Q})$ pour tout $t \in \mathbb{Z}_{\neq 0}$ et tout entier strictement positif n.

On note que $(0, n^3)$ n'est pas un point de torsion de E lorsque δ est sans facteurs carrés. En effet, puisque $(0, n^3) \in E(\mathbb{Q}) - E_0(\mathbb{Q})$, l'ordre $(0, n^3)$ ne peut être impair si son ordre est fini. De plus, puisque le polynôme $f(x)$ est irréductible sur $\mathbb{Q}$ sous l'hypothèse δ sans facteurs carrés, $E(\mathbb{Q})$ ne possède pas de point de torsion d'ordre pair. Il vient donc que le point $(0, n^3)$ est d'ordre infini.

Dans toute la suite, on supposera que δ est sans facteurs carrés, ce qui implique que n et t sont premiers entre eux. Cette condition jouera un rôle important plus tard. D'autre part, il est nécessaire que (1.3) soit une équation de Weierstrass minimale pour E, ce qui par l'algorithme de Tate [45, IV.9], se produit lorsque t n'est pas congru à 1 modulo 4 si $4 \mid n$. Si $4 \nmid n$, l'équation (1.3) définit un modèle minimal pour E si t est premier avec n. L'équation de Weierstrass minimale sera nécessaire pour calculer les contributions locales non archimédiennes de la hauteur canonique.

Pour le cas $4 \mid n$ et $t \equiv 1\,[4]$, on écrit $n = 4m$ et $t = 4k + 1$ avec $m \in \mathbb{Z}_{>0}$ et $k \in \mathbb{Z}$. La courbe elliptique E est isomorphe sur $\mathbb{Q}$ à la courbe

$$E' : y^2 + xy = x^3 + kx^2 - m^2(4k + 1 - 48m^2)x + 64m^6. \tag{1.4}$$

La courbe E' est reliée à E par le changement de variables

$$\begin{aligned} x &= 4x', \\ y &= 8y' + x'. \end{aligned}$$

On remarque que l'équation (1.4) est minimale pour E'. Le changement de variables envoie le point $(0, n^3) \in E(\mathbb{Q})$ sur le point $(0, 8m^3) \in E'(\mathbb{Q})$. Ainsi, si nous voulons montrer la non-divisibilité du point $(0, n^3)$ sur $E(\mathbb{Q})$, il suffit de montrer la non-divisibilité du point $(0, 8m^3)$ sur $E'(\mathbb{Q})$.

1.2 Estimations des périodes

L'objectif de cette partie est de donner une approximation de la période réelle ω_1 et de la période imaginaire ω_2 de E. À noter que pour calculer ω_1 et ω_2, l'équation de Weierstrass définissant E n'a pas besoin d'être minimale. Soit n un entier fixé. La courbe elliptique $E : y^2 = x^3 + tx^2 - n^2(t + 3n^2)x + n^6$ est isomorphe sur $\mathbb{Q}$ à la courbe

$$y^2 = 4g(x),$$

où $g(x) = x^3 - \frac{1}{3}\delta x + \frac{1}{27}(2t + 3n^2)\delta$. Les trois racines réelles e_1, e_2, e_3 de g sont données par $e_i = \alpha_i + \dfrac{t}{3}$ pour tout $i \in \{1, 2, 3\}$ et les périodes ω_1 et ω_2

de E sont (voir [9, 7.3.2])

$$\omega_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{g(x)}} \quad \in \mathbb{R}, \quad \omega_2 = i\int_{e_2}^{e_3} \frac{dx}{\sqrt{|g(x)|}} \quad \in i\mathbb{R}.$$

Pour calculer les approximations de ω_1 et ω_2, nous aurons besoin de distinguer le cas $t > 0$ et le cas $t < 0$.

1.2.1 Le cas $t > 0$

Lorsque $t > 0$, les racines de g vérifient $e_1 < 0 < e_2 < e_3$ car $g(0) > 0$. Une étude élémentaire de la fonction g donne les encadrements suivants lorsque $t \geq 3n^2$:

$$\begin{aligned} -\frac{2}{3}t - n^2 - 2\frac{n^4}{t} \leq e_1 \leq -\frac{2}{3}t - n^2 - \frac{n^4}{t}, \\ \frac{t}{3} \leq e_2 \leq \frac{t}{3} + \frac{n^4}{t}, \\ \frac{t}{3} + n^2 \leq e_3 \leq \frac{t}{3} + n^2 + \frac{n^4}{t}. \end{aligned} \tag{1.5}$$

Lemme 22. *Soit n un entier strictement positif fixé. Lorsque $t \to +\infty$, on a $\frac{\omega_2}{i} \sim \frac{\pi}{\sqrt{t}}$. De plus si $t \geq 100n^2$, on a*

$$\frac{3.11}{\sqrt{t}} \leq \frac{\omega_2}{i} \leq \frac{3.15}{\sqrt{t}}.$$

Démonstration. On remarque que $\frac{\omega_2}{i} = \int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}}$. Si $x \in [e_2, e_3]$, on a $t + n^2 + \frac{n^4}{t} \leq x - e_1 \leq t + 2n^2 + \frac{3n^4}{t}$ par (1.5). Donc

$$\frac{1}{\sqrt{t + 2n^2 + \frac{3n^4}{t}}} \leq \frac{1}{\sqrt{x - e_1}} \leq \frac{1}{\sqrt{t + n^2 + \frac{n^4}{t}}},$$

et alors

$$\frac{\displaystyle\int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_2)(e_3-x)}}}{\sqrt{t + 2n^2 + \frac{3n^4}{t}}} \leq \frac{\omega_2}{i} \leq \frac{\displaystyle\int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_2)(e_3-x)}}}{\sqrt{t + n^2 + \frac{n^4}{t}}}, \tag{1.6}$$

où $\displaystyle\int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_2)(e_3-x)}} = \pi$. De plus, quand $t \to +\infty$ les termes de gauche et de droite de (1.6) sont tous deux équivalents à $\dfrac{\pi}{\sqrt{t}}$. Finalement, lorsque $t \geq 100n^2$, on obtient par (1.6)

$$\frac{3.11}{\sqrt{t}} \leq \frac{\omega_2}{i} \leq \frac{3.15}{\sqrt{t}}.$$

□

Lemme 23. *Si $t \geq 100n^2$, on a*

$$\frac{1.88 + 0.99\log\left(\frac{t}{n^2}\right)}{\sqrt{t}} \leq \omega_1 \leq \frac{5.35 + 1.23\log\left(\frac{t}{n^2}\right)}{\sqrt{t}}.$$

Démonstration. On décompose l'intégrale en deux parties

$$\omega_1^- = \int_{e_1}^{0} \frac{dx}{\sqrt{(x-e_1)(e_2-x)(e_3-x)}}, \omega_1^+ = \int_{0}^{e_2} \frac{dx}{\sqrt{(x-e_1)(e_2-x)(e_3-x)}}.$$

On commence par regarder ω_1^-. Si $x \in [e_1, 0]$, on a $\frac{t}{3} \leq e_2 - x \leq t + n^2 + \frac{3n^4}{t}$ et $\frac{t}{3} + n^2 \leq e_3 - x \leq t + 2n^2 + \frac{3n^4}{t}$ par (1.5). On obtient alors la minoration

$$\begin{aligned}\omega_1^- \sqrt{\left(t + n^2 + \frac{3n^4}{t}\right)\left(t + 2n^2 + \frac{3n^4}{t}\right)} &\geq \int_{e_1}^{0} \frac{dx}{\sqrt{x - e_1}} \\ &\geq 2\sqrt{-e_1} \\ &\geq 2\sqrt{\tfrac{2}{3}t + n^2 + \tfrac{n^4}{t}}.\end{aligned}$$

D'autre part, en utilisant (1.5), on obtient la majoration suivante :

$$\omega_1^- \leq \frac{\displaystyle\int_{e_1}^{0} \frac{dx}{\sqrt{x-e_1}}}{\sqrt{\frac{t}{3}\left(\frac{t}{3} + n^2\right)}} \leq \frac{2\sqrt{-e_1}}{\sqrt{\frac{t}{3}\left(\frac{t}{3} + n^2\right)}} \leq \frac{6}{\sqrt{t}}\sqrt{\frac{2}{3} + \frac{n^2}{t} + \frac{2n^4}{t^2}}.$$

Ainsi lorsque $t \geq 100n^2$, on obtient

$$\frac{1.60}{\sqrt{t}} \leq \omega_1^- \leq \frac{4.94}{\sqrt{t}}.$$

On s'intéresse maintenant à ω_1^+. Si $x \in [0, e_2]$, on a $\frac{2}{3}t + n^2 + \frac{n^4}{t} \leq x - e_1 \leq t + n^2 + \frac{n^4}{t}$ par (1.5). On a alors

$$\frac{J}{\sqrt{t + n^2 + \frac{3n^4}{t}}} \leq \omega_1^+ \leq \frac{J}{\sqrt{\frac{2}{3}t + n^2 + \frac{n^4}{t}}},$$

avec

$$J = \int_0^{e_2} \frac{dx}{\sqrt{(e_2 - x)(e_3 - x)}} = \log\left(\frac{\sqrt{e_3} + \sqrt{e_2}}{\sqrt{e_3} - \sqrt{e_2}}\right).$$

De plus, par (1.5), on a

$$\frac{\frac{4}{3}t + n^2}{n^2 + \frac{n^4}{t}} \leq \frac{\sqrt{e_3} + \sqrt{e_2}}{\sqrt{e_3} - \sqrt{e_2}} \leq \frac{\frac{2}{3}t + n^2 + \frac{2n^4}{t} + 2\sqrt{(\frac{t}{3} + n^2 + \frac{n^4}{t})(\frac{t}{3} + \frac{n^4}{t})}}{n^2 - \frac{n^4}{t}},$$

ce qui implique

$$\frac{\frac{4}{3}t + n^2}{n^2 + \frac{n^4}{t}} \leq \frac{\sqrt{e_3} + \sqrt{e_2}}{\sqrt{e_3} - \sqrt{e_2}} \leq \frac{\frac{4}{3}t + 3n^2 + \frac{4n^4}{t}}{n^2 - \frac{n^4}{t}}.$$

On obtient alors

$$\frac{1}{\sqrt{t + n^2 + \frac{3n^4}{t}}} \log\left(\frac{\frac{4}{3}t + n^2}{n^2 + \frac{n^4}{t}}\right) \leq \omega_1^+ \leq \frac{1}{\sqrt{\frac{2}{3}t + n^2 + \frac{n^4}{t}}} \log\left(\frac{\frac{4}{3}t + 3n^2 + \frac{4n^4}{t}}{n^2 - \frac{n^4}{t}}\right).$$

Supposons maintenant que $t \geq 100n^2$. On a

$$\begin{aligned}\omega_1^+ &\leq \frac{1}{\sqrt{\frac{2}{3}t + n^2 + \frac{n^4}{t}}} \left(\log(t) + \log\left(\frac{4}{3}\right) + \log\left(1 + \frac{3n^2}{t} + \frac{4n^4}{t^2}\right)\right. \\ &\quad \left. - \log\left(n^2 - \frac{n^4}{t}\right)\right) \\ &\leq \frac{0.41 + 1.23\log\left(\frac{t}{n^2}\right)}{\sqrt{t}}\end{aligned}$$

et

$$\omega_1^+ \geq \frac{1}{\sqrt{t + n^2 + \frac{3n^4}{t}}} \log\left(\frac{4t}{3(n^2 + \frac{n^4}{t})}\right) \geq \frac{0.28 + 0.99\log\left(\frac{t}{n^2}\right)}{\sqrt{t}}.$$

On obtient finalement la conclusion attendue.

□

Remarque. Une étude numérique suggère que ω_1 doit être équivalent à $\frac{\log\left(\frac{t}{n^2}\right)}{\sqrt{t}}$ lorsque $t \to +\infty$.

1.2.2 Le cas $t < 0$

De nouveau, on utilise le fait que E est isomorphe à la courbe $y^2 = 4g(x)$. Une étude élémentaire de la fonction g nous donne les estimations suivantes lorsque $t \leq -3n^2$:

$$\begin{array}{rcl} \frac{t}{3} + \frac{2n^4}{t} & \leq e_1 \leq & \frac{t}{3} + \frac{n^4}{t}, \\ \frac{t}{3} + n^2 + \frac{2n^4}{t} & \leq e_2 \leq & \frac{t}{3} + n^2 + \frac{n^4}{t}, \\ -\frac{2t}{3} - n^2 & \leq e_3 \leq & -\frac{2t}{3}. \end{array} \tag{1.7}$$

Lemme 24. *Lorsque $t \to -\infty$, on a $\omega_1 \sim \frac{\pi}{\sqrt{|t|}}$. De plus, pour $t \leq -100n^2$ on a*

$$\frac{3.14}{\sqrt{|t|}} \leq \omega_1 \leq \frac{3.15}{\sqrt{|t|}}.$$

Démonstration. Si $x \in [e_1, e_2]$, alors $|t| - 2n^2 + \frac{n^4}{|t|} \leq e_3 - x \leq |t| + \frac{2n^4}{|t|}$ par (1.7). Donc

$$\frac{1}{\sqrt{|t| + \frac{2n^4}{|t|}}} \leq \frac{1}{\sqrt{e_3 - x}} \leq \frac{1}{\left|\sqrt{|t|} - \frac{n^2}{\sqrt{|t|}}\right|}.$$

On obtient donc

$$\frac{J}{\sqrt{|t| + \frac{2n^4}{|t|}}} \leq \omega_1 \leq \frac{J}{\left|\sqrt{|t|} - \frac{n^2}{\sqrt{|t|}}\right|},$$

avec

$$J = \int_{e_1}^{e_2} \frac{dx}{\sqrt{(x - e_1)(e_2 - x)}} = \pi.$$

Puisque $\frac{\pi}{\sqrt{|t| + \frac{2n^4}{|t|}}}$ et $\frac{\pi}{\sqrt{|t|} - \frac{n^2}{\sqrt{|t|}}}$ sont tous deux équivalents à $\frac{\pi}{\sqrt{|t|}}$ lorsque $t \to -\infty$, on en déduit que $\omega_1 \underset{t \to -\infty}{\sim} \frac{\pi}{\sqrt{|t|}}$. D'autre part, $t \leq -100n^2$, on obtient

$$\frac{3.14}{\sqrt{|t|}} \leq \omega_1 \leq \frac{3.15}{\sqrt{|t|}}.$$

□

Lemme 25. *Si $t \leq -100n^2$, on a*

$$\frac{\omega_2}{i} \geq \frac{0.39 + \log\left(\frac{|t|}{n^2}\right)}{\sqrt{|t|}}.$$

Démonstration. Remarquons que $e_2 < 0 < e_3$ comme $g(0) < 0$ si $t \leq -100n^2$. Pour encadrer ω_2, on a besoin de décomposer l'intégrale en deux parties :

$$\frac{\omega_2}{i} = \underbrace{\int_{e_2}^{0} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}}}_{W^-} + \underbrace{\int_{0}^{e_3} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}}}_{W^+}.$$

On commence par estimer W^-. Si $x \in [e_2, 0]$, on obtient grâce à (1.7)

$$-\frac{2}{3}t - n^2 \leq e_3 - x \leq -t - n^2 - \frac{2n^4}{t}.$$

Donc

$$\frac{L}{\sqrt{-t-n^2-\frac{2n^4}{t}}} \leq W^- \leq \frac{L}{\sqrt{-\frac{2}{3}t-n^2}},$$

avec

$$L = -\int_0^{e_2} \frac{dx}{\sqrt{(x-e_1)(x-e_2)}} = -\log(e_2-e_1) + \log\big(-e_1-e_2+\sqrt{e_1e_2}\big).$$

De plus, par (1.7), on a

$$-\log\left(n^2 - \frac{n^4}{t}\right) + \log\left(-\frac{2}{3}t - n^2 - \frac{2n^4}{t}\right) \leq L.$$

Pour $t \leq -100n^2$, on obtient

$$\begin{aligned} W^-\sqrt{-t-n^2-\tfrac{2n^4}{t}} &\geq -\log\left(n^2-\frac{n^4}{t}\right) + \log\left(-\frac{2}{3}t-n^2-\frac{2n^4}{t}\right) \\ &\geq -\log(n^2) - \log\left(\tfrac{99}{100}\right) + \log(|t|) + \log\left(\tfrac{197}{300}\right), \end{aligned}$$

ce qui nous donne

$$W^- \geq \frac{\log\left(\frac{|t|}{n^2}\right) - 0.42}{\sqrt{|t|}}. \tag{1.8}$$

Si $x \in [0, e_3]$, on obtient par (1.7)

$$\begin{aligned} -\frac{t}{3} - \frac{n^4}{t} \leq x - e_1 \leq -t - \frac{2n^4}{t}, \\ -\frac{t}{3} - n^2 - \frac{n^4}{t} \leq x - e_2 \leq -t - n^2 - \frac{2n^4}{t}. \end{aligned}$$

Donc

$$W^+\sqrt{\left(-t-\tfrac{2n^4}{t}\right)\left(-t-n^2-\tfrac{n^4}{t}\right)} \geq 2\sqrt{e_3},$$

ce qui nous donne

$$W^+ \geq \frac{\sqrt{-\frac{2}{3}t-n^2}}{\sqrt{(-t-\frac{2n^4}{t})(-t-n^2-\frac{n^4}{t})}} \geq \frac{\sqrt{|t|}\sqrt{\frac{2}{3}-\frac{n^2}{|t|}}}{|t|\sqrt{(1+\frac{2n^4}{|t|^2})^2}}.$$

On obtient alors, pour $t \leq -100n^2$

$$W^+ \geq \frac{0.81}{\sqrt{|t|}}. \tag{1.9}$$

Finalement, en additionnant les deux inégalités (1.8) et (1.9), on obtient

$$\frac{\omega_2}{i} \geq \frac{0.39+\log\left(\frac{|t|}{n^2}\right)}{\sqrt{|t|}}.$$

□

Remarque. Pour $t<0$, on a seulement donné une minoration de $\frac{\omega_2}{i}$ puisqu'il n'est pas nécessaire d'avoir une majoration pour l'estimation de la hauteur.

1.3 Estimations sur les hauteurs

Nous avons besoin d'estimer la hauteur des points de $E(\mathbb{Q})$. Pour ce faire, nous allons décomposer la hauteur canonique en somme de contributions locales. Suivant les conventions, il y a différentes manières de décomposer la hauteur en somme de contributions locales. Cependant dans cette section, un soin particulier a été mis durant le calcul des contributions locales de la hauteur pour s'assurer que leur somme concorde avec la définition de la hauteur canonique.

1.3.1 Minoration de la hauteur

On veut montrer que le point $(0,n^3)$ n'est pas divisible sur E, c'est-à-dire qu'il n'existe pas de point $P=(\alpha,\beta)\in E(\mathbb{Q})$ et d'entier $\ell\geq 2$ tels que $\ell P=(0,n^3)$. L'objectif de cette partie est de trouver, si un tel point existe, une minoration de la hauteur de P. Puisque $(0,n^3)\in E(\mathbb{Q})-E_0(\mathbb{Q})$, le point P appartient nécessairement $E(\mathbb{Q})-E_0(\mathbb{Q})$ et ℓ doit être impair (voir section 1.1).

Lemme 26. *Soit $F : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ une courbe elliptique définie sur $\mathbb{Q}$ avec $a_i \in \mathbb{Z}$ pour tout $i \in \{1, 2, 3, 4, 6\}$. Soit $P \in F(\mathbb{Q})$ un point d'ordre infini tel que mP soit un point entier pour un certain $m \geq 1$. Alors P est un point entier de F.*

Démonstration. Une preuve de ce lemme est effectuée dans [1]. On écrit $mP = (\alpha, \beta)$ avec $\alpha, \beta \in \mathbb{Z}$ et $P = (x, y)$ avec $x, y \in \mathbb{Q}$. Soient ψ_m, ϕ_m les m-ièmes polynômes de division. On rappelle que ϕ_m est un polynôme unitaire de $\mathbb{Z}[X]$ de degré m^2 et ψ_m^2 est un polynôme de $\mathbb{Z}[X]$ de degré $m^2 - 1$ (pour plus de détails voir [1], Section 2). On a

$$\frac{\phi_m(x)}{\psi_m^2(x)} = \alpha.$$

On obtient alors que x est une racine du polynôme $\phi_m(X) - \alpha\psi_m^2(X)$. Puisque $\phi_m(X) - \alpha\psi_m^2(X)$ est unitaire dans $\mathbb{Z}[X]$ et $x \in \mathbb{Q}$, on en déduit que $x \in \mathbb{Z}$ puis que $y \in \mathbb{Z}$. Donc P est un point entier. □

Le lemme 26 implique que si $(0, n^3)$ est le multiple d'un point rationnel P alors $P \in E(\mathbb{Z})$. D'autre part $(0, n^3)$ est un point singulier modulo p pour tout nombre premier $p \mid n$. Cela implique que P est singulier modulo p pour tout $p \mid n$ puisque le multiple d'un point non singulier est toujours non singulier. Si $p \mid n$, l'unique point singulier modulo p est $(0, 0)$: on a alors que $p \mid \alpha$. Cette remarque est utilisée dans les lemmes 27, 28 et la proposition 32.

Lemme 27. *Soit $P = (\alpha, \beta) \in E(\mathbb{Z}) - E_0(\mathbb{Z})$ tel qu'il existe un entier $\ell \geq 2$ avec $\ell P = (0, n^3)$. Si $t \geq 2n^4$ alors $|\beta| \geq n\sqrt{2t}$.*

Démonstration. Supposons que $t \geq 2n^4$ et $n \geq 2$. On rappelle que $\alpha_1, \alpha_2, \alpha_3$ sont les trois racines réelles de $f(x) = x^3 + tx^2 - n^2(t + 3n^2)x + n^6$ vérifiant $\alpha_1 < 0 < \alpha_2 < \alpha_3$. En étudiant la fonction f, on a si $t \geq 2n^4$:

$$-n^2 - t - 1 < \alpha_1 < -n^2 - t \quad \text{et} \quad 0 < \alpha_2 < 1.$$

Puisque $P \in E(\mathbb{Q}) - E_0(\mathbb{Q})$, on a $\alpha_1 < \alpha < \alpha_2$, et alors $\alpha \in [-n^2 - t, -1]$. De plus, puisque $p \mid \alpha$ pour tout nombre premier $p \mid n$, on obtient $\alpha \leq -2$ et alors

$$\begin{aligned} f(\alpha) &\geq \min(f(-n^2 - t), f(-2)) \\ &\geq \min\left(2n^4t + 3n^6, (2n^2 + 4)t + n^6 + 6n^4 - 8\right) \\ &\geq 2n^2t. \end{aligned}$$

Donc $|\beta| \geq n\sqrt{2t}$. Lorsque $n = 1$, on a

$$f(\alpha) \geq \min(f(-t - 1), f(-1)) = 2t + 3,$$

donc $|\beta| \geq \sqrt{2t + 3} \geq \sqrt{2t}$. □

Lemme 28. *On suppose que $t \leq -2n^4$. Alors*

$$|\beta| \geq \begin{cases} \sqrt{2|t|} & \text{if } n = 2, \\ n\sqrt{|t|} & \text{if } n \geq 3. \end{cases}$$

Démonstration. On utilise un argument similaire au cas $t \geq n^4$ (lemme 27). □

Remarque. On suppose $n = 1$. Si $t \leq -2$, le point $(0, 1)$ est le seul point entier sur $E(\mathbb{Q}) - E_0(\mathbb{Q})$ car $-1 < \alpha_1 < \alpha_2$. Donc $(0, 1)$ n'est pas divisible. Pour $t = -1$, il est facile de montrer que le point $(0, 1)$ n'est pas divisible. Ainsi lorsque t est négatif, on peut supposer que $n \geq 2$.

Exemple 29. Pour $t = -2$, l'équation de E est de la forme

$$E\colon y^2 = x^3 - 2x^2 - x + 1.$$

À l'aide de la fonction `ellrank` du logiciel PARI/GP [48] on établit que le rang de E est 1. Le point $(0, 1)$ est non-divisible par l'argument de la remarque précédente. De plus, on remarque que $E(\mathbb{Q})$ est sans torsion donc $E(\mathbb{Q}) = \langle (0, 1) \rangle$.

Pour minorer la hauteur canonique d'un point entier de E, on utilise la décomposition de la hauteur canonique en contributions locales (voir [43, théorème 5.2], [8, 7.5.7]). Soit $P = (\alpha, \beta) \in E(\mathbb{Q})$ un point entier. On a

$$\widehat{h}(P) = \sum_{p \leq \infty} \lambda_p(P),$$

où la somme parcourt l'ensemble des places de $\mathbb{Q}$. À noter que cette somme est finie : en effet $\lambda_p(P) \neq 0$ seulement pour un nombre fini de places p. On rappelle les définitions des λ_p pour les places finies p dans la définition/proposition 30 et λ_∞ dans la définition/proposition 33. Pour ce faire, on pose

$$\begin{aligned} A &= 3\alpha^2 + 2t\alpha - n^2(t + 3n^2), \\ B &= 2\beta, \\ C &= 3\alpha^4 + 4t\alpha^3 - 6n^2(t + 3n^2)\alpha^2 + 12n^6\alpha - n^4(t^2 + 2n^2t + 9n^4), \\ D &= \operatorname{pgcd}(A, B), \\ c_4 &= 16\delta. \end{aligned}$$

Définition-Proposition 30. *([43, Theorem 5.2],[8, 7.5.6]) Soit p un nombre premier. La contribution locale non archimédienne $\lambda_p(P)$ est non nulle si*

$p \mid D$. Si $p \mid D$, on pose $m_p = \min\left(\frac{v_p(\Delta)}{2}, v_p(B)\right)$, la contribution locale est donnée par

$$\lambda_p(P) = \begin{cases} -\dfrac{m_p(v_p(\Delta) - m_p)}{2v_p(\Delta)} \log(p) & \text{si } p \nmid c_4, \\ -\dfrac{v_p(B)}{3} \log(p) & \text{si } p \mid c_4 \text{ et } v_p(C) \geq 3v_p(B), \\ -\dfrac{v_p(C)}{8} \log(p) & \text{sinon,} \end{cases}$$

où v_p est la valuation p-adique.

Lemme 31. *On suppose que $4 \nmid n$ où $t \not\equiv 1[4]$. Si $p \nmid 2n$, alors $\lambda_p(P) = 0$.*

Démonstration. Soit $p \mid D$. On suppose que $p \nmid n$ et $p \neq 2$. Premièrement, on a $4A^2 = B^2(9\alpha + 3t) + 4\delta(\alpha^2 - n^2\alpha + n^4)$. Puisque δ est sans facteurs carrés, on obtient que $p \mid (\alpha^2 - n^2\alpha + n^4)$. Nous avons également

$$B^2 = 4(\alpha^2 - n^2\alpha + n^4)(\alpha + t + n^2) - 4n^4(3\alpha + t)$$

donc $p \mid (3\alpha + t)$. D'autre part, p divise le résultant A et B^2, vu comme un polynôme de $\mathbb{Z}[\alpha]$, qui est égal à $\Delta = 16n^4\delta^2$. Donc $p \mid \delta$. De plus,

$$27B^2 = 4(3\alpha + t)^3 - 4\delta(9\alpha + t - 3n^2),$$

ce qui implique que $p \mid (9\alpha + t - 3n^2)$. Puisque $(9\alpha + t - 3n^2) = 3(3\alpha + t) - (2t + 3n^2)$, on obtient que $p \mid (2t + 3n^2)$. Or $4\delta = (2t + 3n^2)^2 + 27n^4$. Il vient que $p = 3$ donc δ possède un facteur carré, ce qui donne une contradiction. □

Proposition 32. *Soit $P = (\alpha, \beta)$ un point entier sur E tel que $\ell P = (0, n^3)$ pour un certain entier $\ell \geq 1$. Alors on a l'inégalité suivante :*

$$\sum_{p < \infty} \lambda_p(P) \geq -\frac{1}{2}\log(n) - \frac{1}{3}\log(2).$$

Démonstration. Par le lemme 31, il suffit de calculer les contributions locales pour $p \mid 2n$. Pour $p \mid n$, on commence par supposer que $p \neq 2$. Soit $m = v_p(n)$. Puisque δ est sans facteurs carrés, on a $p \nmid c_4$ et $v_p(\Delta) = 4m$. On pose $m_p = \min(2m, v_p(B))$. Par la définition/proposition 30, la contribution locale de P est donnée par

$$\lambda_p(P) = -\frac{m_p(4m - m_p)}{8m} \log(p).$$

On conclut facilement que

$$\lambda_p(P) \ \geq -\frac{m}{2}\log(p) \ \geq -\frac{1}{2}\log(p^m).$$

On veut maintenant minorer la 2-contribution locale $\lambda_2(P)$. Puisque $2 \mid c_4$, elle est donnée par

$$\lambda_2(P) = \begin{cases} -\dfrac{v_2(B)}{3}\log(2) & \text{si } v_2(C) \geq 3v_2(B), \\ -\dfrac{v_2(C)}{8}\log(2) & \text{sinon.} \end{cases}$$

- Si $2 \nmid n$ alors $v_2(B) = 1$, donc $\lambda_2(P) \geq -\dfrac{1}{3}\log(2)$. Supposons maintenant que $2 \mid n$ et $m = v_2(n)$. Si $m \in \{1, 2\}$ il est facile de vérifier que $\lambda_2(P) \geq -\dfrac{1}{2}\log(2^m) - \dfrac{1}{3}\log(2)$. On peut donc supposer que $m \geq 3$.
- Si $v_2(\alpha) < m$ alors $v_2(B) = 1 + v_2(\alpha)$; dans ce cas on a $\lambda_2(P) \geq \dfrac{-m}{3}\log(2)$ si $v_2(C) \geq 3v_2(B)$, sinon $\lambda_2(P) \geq -\dfrac{m}{2}\log(2)$.
- Si $m \leq v_2(\alpha) < \frac{4m-2}{3}$ alors $v_2(B) = 1 + v_2(\alpha)$ et $v_2(C) = 3v_2(\alpha) + 2$; dans ce cas on a $\lambda_2(P) = -\dfrac{3v_2(\alpha)+2}{8}\log(2) \geq -\dfrac{1}{2}\log(2^m)$.
- Si $v_2(\alpha) = \dfrac{4m-2}{3}$ ce qui est possible seulement si $m \equiv 2[3]$ alors $v_2(C) > 4m$ et $v_2(B) = \dfrac{4m+1}{3}$. Dans ce cas on obtient que $\lambda_2(P) = -\dfrac{4m+1}{9}\log(2) \geq -\dfrac{m}{2}\log(2)$.
- Si $v_2(\alpha) > \dfrac{4m-2}{3}$, alors $v_2(C) = 4m$ et $3v_2(B) > 4m$; dans ce cas on a $\lambda_2(P) \geq -\dfrac{1}{2}\log(2^m)$.

Finalement, on conclut en additionnant toutes les contributions locales non archimédiennes. □

On étudie maintenant la contribution locale archimédienne.

Définition-Proposition 33. *([8, 7.5.7]) Soit $P = (\alpha, \beta) \in E(\mathbb{Q})$. Soit z le logarithme elliptique de P. Soient $\mu = \dfrac{2\pi}{\omega_1}$, $s = \mu\mathrm{Re}(z)$, $q = \exp\left(\dfrac{2i\pi\omega_2}{\omega_1}\right)$, et*

$$\theta = \sum_{k=0}^{\infty} \sin((2k+1)s)(-1)^k q^{\frac{k(k+1)}{2}}.$$

Alors la contribution locale archimédienne est donnée par

$$\lambda_\infty(P) = \frac{1}{32}\log\left|\frac{\Delta}{q}\right| - \frac{1}{4}\log|\theta| + \frac{1}{8}\log\left|\frac{\alpha^3 + \frac{b_2}{4}\alpha^2 + \frac{b_4}{2}\alpha + \frac{b_6}{4}}{\mu}\right|$$

où $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$ *et* a_1, a_2, a_3, a_4 *et* a_6 *sont définis de la même manière que dans le lemme 26.*

Proposition 34. *On suppose que* $4 \nmid n$ *ou* $t \not\equiv 1[4]$ *et que* $\ell P = (0, n^3)$ *pour un certain entier* ℓ. *Si* $t \geq \max(100n^2, 2n^4)$, *on a*

$$\lambda_\infty(P) \geq \frac{13}{80}\log(t) + \frac{3}{8}\log(n) + 0.30.$$

Si $t \leq \min(-100n^2, -2n^4)$, *on a*

$$\lambda_\infty(P) \geq \frac{3}{16}\log(|t|) + \frac{3}{8}\log(n) + 0.27.$$

Démonstration. On commence par remarquer que

$$|\theta| \leq \sum_{k=0}^{\infty} q^{\frac{k(k+1)}{2}} \leq \frac{1}{1-q}. \tag{1.10}$$

Pour trouver une minoration de $\lambda_\infty(P)$, il nous faut majorer q. Si $t \geq 100n^2$, par les lemmes 22 et 23, on a

$$\frac{2i\pi\omega_2}{\omega_1} \leq \frac{-3.11 \times 2\pi}{5.35 + 1.23\log\left(\frac{t}{n^2}\right)} \leq \frac{-15.88}{\log(\frac{t}{n^2})}$$

donc

$$q \leq \exp\left(\frac{-15.88}{\log(\frac{t}{n^2})}\right) \leq 1 - \frac{4.3}{\log(\frac{t}{n^2})}. \tag{1.11}$$

Dans un premier temps, par la définition de Δ on a

$$\frac{1}{32}\log(\Delta) = \frac{1}{32}\log\left(16n^4(t^2 + 3n^2t + 9n^4)^2\right) \geq \frac{1}{8}\log(t) + \frac{1}{8}\log(n) + \frac{1}{8}\log(2).$$

Dans un second temps, à l'aide de (1.11) et de (1.10) on obtient

$$\frac{1}{32}\log\left|\frac{1}{q}\right| \geq \frac{1}{32}\log\left(\exp\left(\frac{15.88}{\log(\frac{t}{n^2})}\right)\right) \geq \frac{15.88}{32\log(\frac{t}{n^2})},$$

$$-\frac{1}{4}\log|\theta| \geq -\frac{1}{4}\log\left|\frac{1}{1-q}\right| \quad \geq \quad \frac{1}{4}\log(4.3) - \frac{1}{4}\log\log\left(\frac{t}{n^2}\right),$$

et par le lemme 23,

$$\begin{aligned}-\frac{1}{8}\log(\mu)=\frac{1}{8}\log\left(\frac{\omega_1}{2\pi}\right) &\geq -\frac{1}{8}\log(2\pi)+\frac{1}{8}\log\left(\frac{1.88+0.99\log\left(\frac{t}{n^2}\right)}{\sqrt{t}}\right),\\ &\geq -\frac{1}{16}\log(t)-\frac{1}{8}\log(2\pi)+\frac{1}{8}\log\log\left(\frac{t}{n^2}\right)\\ &\quad +\frac{1}{8}\log(0.99).\end{aligned}$$

De plus, on a

$$\frac{1}{8}\log(2)+\frac{1}{4}\log(4.3)-\frac{1}{8}\log(2\pi)+\frac{1}{8}\log(0.99)\geq 0.22.$$

Finalement, en utilisant la définition/proposition 33 et le fait que

$$\alpha^3+\frac{b_2}{4}\alpha^2+\frac{b_4}{2}\alpha+\frac{b_6}{4}=\beta^2,$$

on obtient la minoration suivante de $\lambda_\infty(P)$:

$$\begin{aligned}\lambda_\infty(P) &\geq \frac{1}{16}\log(t)-\frac{1}{8}\log\log\left(\frac{t}{n^2}\right)+\frac{15.88}{32\log(\frac{t}{n^2})}\\ &\quad +\frac{1}{4}\log|\beta|+\frac{1}{8}\log(n)+0.22.\end{aligned}$$

D'autre part, par le lemme 27, pour $t\geq n^4$ on a $|\beta|\geq n\sqrt{2t}$.
Pour $t\geq \max(n^4,100n^2)$, on obtient

$$\lambda_\infty(P)\geq\frac{13}{80}\log(t)+\frac{3}{8}\log(n)+0.30.$$

Lorsque t est strictement négatif, on procède de la même manière pour minorer $\lambda_\infty(P)$. Si $t\leq -100n^2$, on a par les lemmes 24 and 25

$$\frac{2i\pi\omega_2}{\omega_1}\leq\frac{-2\pi\left(0.39+\log\left(\frac{|t|}{n^2}\right)\right)}{3.15}\leq-\frac{2\pi}{3.15}\log\left(\frac{|t|}{n^2}\right),$$

et

$$q\leq\exp\left(-\frac{2\pi}{3.15}\log\left(\frac{|t|}{n^2}\right)\right)\leq 0.0002. \tag{1.12}$$

D'une part, par la définition de Δ on a

$$\frac{1}{32}\log(\Delta) \geq \frac{1}{8}\log(|t|)+\frac{1}{8}\log(n)+\frac{1}{8}\log(2)+\frac{1}{32}\log\left(1-\frac{3}{100}\right).$$

D'autre part, à l'aide de (1.12) et de (1.10) on obtient

$$\frac{1}{32}\log\left|\frac{1}{q}\right| \geq \frac{1}{32}\log\exp\left(\frac{2\pi}{3.15}\log\left(\frac{|t|}{n^2}\right)\right) \geq 0.28,$$

et

$$-\frac{1}{4}\log|\theta| \geq -\frac{1}{4}\log\left|\frac{1}{1-q}\right| \geq -\frac{1}{4}\log\left(\frac{1}{1-0.0002}\right),$$

et, par le lemme 24,

$$\begin{aligned}-\frac{1}{8}\log(\mu) &\geq -\frac{1}{8}\log(2\pi)+\frac{1}{8}\log\left(\frac{3.14}{\sqrt{|t|}}\right)\\ &\geq -\frac{1}{16}\log(|t|)-\frac{1}{8}\log(2\pi)+\frac{1}{8}\log(3.14).\end{aligned}$$

De plus, on a

$$\frac{1}{8}\log(2)+\frac{1}{8}\log(3.14)-\frac{1}{8}\log(2\pi)+\frac{1}{4}\log(1-0.0002)+0.28 \geq 0.27.$$

On obtient alors

$$\lambda_\infty(P) \geq \frac{1}{16}\log(|t|)+\frac{1}{4}\log|\beta|+\frac{1}{8}\log(n)+0.27.$$

De plus, par le lemme 28, si $t \leq -2n^4$, on a $|\beta| \geq n\sqrt{|t|}$.
Si $t \leq \min(-2n^4, -100n^2)$, on obtient

$$\lambda_\infty(P) \geq \frac{3}{16}\log(|t|)+\frac{3}{8}\log(n)+0.27.$$

□

Théorème 35. *On suppose que $4 \nmid n$ et $t \not\equiv 1[4]$. Soit P un point entier de E tel que $\ell P = (0, n^3)$ pour un certain entier $\ell \geq 2$. Si $t \geq \max(100n^2, 2n^4)$, on a*

$$\widehat{h}(P) \geq \frac{13}{80}\log(t)-\frac{1}{8}\log(n)+0.09.$$

Pour $t \leq \min(-100n^2, -2n^4)$, on a

$$\widehat{h}(P) \geq \frac{3}{16}\log(|t|)-\frac{1}{8}\log(n).$$

Démonstration. Il suffit d'additionner les inégalités obtenues dans la proposition 32 et la proposition 34. □

Par des arguments similaires, on obtient le résultat suivant pour $t = 4k+1$ et $n = 4m$.

Proposition 36. *Si $P \in E'(\mathbb{Q})$ est un point entier tel que $\ell P = (0, 8m^3)$ pour un certain entier $\ell \geq 1$, alors les inégalités suivantes sont vérifiées :*

$$\sum_{p<\infty} \lambda_p(P) \geq -\frac{1}{2}\log(m) \geq -\frac{1}{2}\log(n) + \log(2).$$

Proposition 37. *Soit $P \in E'(\mathbb{Q})$ un point entier tel que $\ell P = (0, 8m^3)$ pour un certain $\ell \geq 2$. Si $t \geq \max(n^4, 100n^2)$, on a*

$$\lambda_\infty(P) \geq \frac{13}{80}\log(t) + \frac{3}{8}\log(n) - \frac{5}{8}\log(2) + 0.04.$$

Si $t \leq \min(-100n^2, -2n^4)$, on a

$$\lambda_\infty(P) \geq \frac{3}{16}\log(|t|) + \frac{3}{8}\log(n) - \frac{3}{4}\log(2) + 0.10.$$

À nouveau après sommation des inégalités obtenues dans les propositions 36 et 37, on obtient le résultat suivant.

Théorème 38. *Soit P un point entier de E' tel que $\ell P = (0, 8m^3)$ pour un certain $\ell \geq 2$. Si $t \geq \max(100n^2, 2n^4)$, on a*

$$\widehat{h}(P) \geq \frac{13}{80}\log(t) + \frac{3}{8}\log(n) + 0.04.$$

Si $t \leq \min(-100n^2, -2n^4)$, on a

$$\widehat{h}(P) \geq \frac{3}{16}\log(|t|) + \frac{1}{4}\log(n) + 0.10.$$

1.3.2 Majoration de la hauteur

On souhaite maintenant majorer la hauteur canonique du point $(0, n^3)$. Pour ce faire nous allons utiliser l'encadrement de la différence entre la hauteur naïve et la hauteur canonique établi par Silverman [44, théorème 1.1] :

Théorème 39. *Soit $E/\mathbb{Q}$ une courbe elliptique donnée par une équation de Weierstrass de la forme :*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les $a_i \in \mathbb{Z}$ *pour tout* $i \in \{1,2,3,4,6\}$. *On note* $b_2 = a_1^2 + 4a_2$ *et on pose*

$$\widehat{\mu}(E) = \frac{1}{12}h(\Delta) + \frac{1}{12}h_\infty(j) + \frac{1}{2}h_\infty\left(\frac{b_2}{12}\right) + \frac{1}{2}\log(\nu),$$

où $\nu = \begin{cases} 2 & \text{si } b_2 \neq 0, \\ 1 & \text{si } b_2 = 0. \end{cases}$ *Alors pour tout* $P \in E(\overline{\mathbb{Q}})$, *on a*

$$-\frac{1}{24}h(j) + \widehat{\mu}(E) - 0.975 \leq \widehat{h}(P) - \frac{1}{2}h(P) \leq \widehat{\mu}(E) + 1.07,$$

où pour $x \in \mathbb{Q}$, $h_\infty(x) = \max(\log|x|, 0)$.

Proposition 40. *Si* $|t| \geq 100n^2$, *l'inégalité suivante est satisfaite*

$$\widehat{h}((0,n^3)) \leq \log(|t|) + 1.57.$$

Démonstration. On utilise le théorème 39. Soit $P \in E(\mathbb{Q})$. On a la majoration suivante

$$\widehat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{12}h(\Delta) + \frac{1}{12}h_\infty(j) + \frac{1}{2}h_\infty\left(\frac{b_2}{12}\right) + \frac{1}{2}\log(2) + 1.07$$

où $h(P) = h(x(P))$ est la hauteur logarithmique sur $\mathbb{Q}$, $h_\infty(x) = \max(\log|x|, 0)$ et b_2 est défini de la même manière que dans la définition/proposition 33. Puisque $h((0,n^3)) = 0$, dans notre situation, nous avons

$$\begin{aligned}
\widehat{h}((0,n^3)) &\leq \frac{1}{12}\log(16n^4(t^2+3n^2t+9n^4)^2) + \frac{1}{12}\log\left(\frac{256}{n^4}(t^2+3n^2t+9n^4)\right) \\
&\quad + \frac{1}{2}\log\left(\frac{|t|}{3}\right) + \frac{1}{2}\log(2) + 1.07 \\
&\leq \frac{1}{4}\log(t^2+3n^2t+9n^4) + \frac{1}{2}\log(|t|) + 1.561 \\
&\leq \log(|t|) + \frac{1}{4}\log\left(1 + \frac{3n^2}{|t|} + \frac{9n^4}{t^2}\right) + 1.561.
\end{aligned}$$

Finalement, lorsque $|t| \geq 100n^2$, on obtient

$$\widehat{h}((0,n^3)) \leq \log(|t|) + 1.57.$$

□

Remarque. On remarque que la majoration donnée dans la proposition 40 est indépendante de n. En réalité, cette borne n'est pas optimale. Une étude numérique nous fait penser que $\widehat{h}((0,n^3))$ devrait être équivalent à $\frac{1}{2}\log\left(\frac{|t|}{n^2}\right)$ lorsque $|t| \to +\infty$. De plus le théorème de Silverman ([40]) nous assure que pour tout $n \in \mathbb{N}^*$, $\dfrac{\widehat{h}((0,n^3))}{\log(|t|)} = O(1)$ lorsque $|t| \to +\infty$.

Par un argument similaire à la proposition 40, on obtient le résultat suivant.

Proposition 41. *Pour le cas $t = 4k + 1$, $n = 4m$. Si $|t| \geq 100n^2$, on a*

$$\widehat{h}((0, 8m^3)) \leq \log(|t|) + 0.19.$$

1.4 Résultats principaux

Proposition 42. *On suppose que $y^2 = f(x)$ est un modèle de Weierstrass minimal pour E lorsque δ est sans facteurs carrés (ce qui se produit lorsque $t \not\equiv 1\,[4]$ quand $4 \mid n$). On suppose également que $|t| \geq \max(100n^2, 2n^4)$. Alors le point $(0, n^3)$ est non-divisible.*

Démonstration. On suppose que t est positif. Soit P un point de $E(\mathbb{Q}) - E_0(\mathbb{Q})$ et $\ell \geq 2$ tel que $\ell P = (0, n^3)$. Par le lemme 26, P est un point entier. Par le théorème 35 on sait que $\widehat{h}(P) \geq \frac{13}{80}\log(t) - \frac{1}{8}\log(n) + 0.06$ et par la proposition 40, on a $\widehat{h}((0, n^3)) \leq \log(t) + 1.57$. On remarque que P est un point d'ordre infini et que par conséquent $\widehat{h}(P) \neq 0$. Puisque $\widehat{h}$ est quadratique, on a

$$\begin{aligned} \ell^2 = \frac{\widehat{h}((0, n^3))}{\widehat{h}(P)} &\leq \frac{\log(t) + 1.57}{\frac{13}{80}\log(t) - \frac{1}{8}\log(n) + 0.06} \\ &\leq \frac{80}{13} + \frac{\frac{2}{3}\log(n) + 1.21}{\frac{13}{80}\log(t) - \frac{1}{8}\log(n) + 0.06} \\ &\leq 8.6 \end{aligned}$$

donc $\ell \leq 2$. Cependant on a montré en début de section 1.3.1 que ℓ est impair, donc le point $(0, n^3)$ n'est pas divisible.

Supposons maintenant que t est négatif. On a par un argument similaire (voir théorème 35 et proposition 40),

$$\begin{aligned} \ell^2 &\leq \frac{\log(|t|) + 1.57}{\frac{3}{16}\log(|t|) - \frac{1}{8}\log(n)} \\ &\leq 5.34 + \frac{\frac{2}{3}\log(n) + 1.57}{\frac{3}{16}\log(|t|) - \frac{1}{8}\log(n)} \\ &\leq 8.85. \end{aligned}$$

De nouveau, on obtient $\ell \leq 2$ ce qui est impossible. Il vient que le point $(0, n^3)$ n'est pas divisible. □

En utilisant le théorème 38 et la proposition 41, on obtient le résultat suivant.

Proposition 43. *On suppose $n = 4m$ et $t = 4k+1$, avec $m \in \mathbb{Z}_{>0}$ et $k \in \mathbb{Z}$. Si δ est sans facteurs carrés, on suppose également que $|t| \geq \max(100n^2, 2n^4)$. Alors le point $(0, n^3)$ n'est pas divisible sur E.*

En combinant les propositions 42 et 43, on obtient le résultat principal de ce chapitre.

Théorème 44. *On suppose que $|t| \geq \max(100n^2, 2n^4)$, et que δ est sans facteurs carrés. Alors le point $(0, n^3)$ n'est pas divisible sur E.*

Exemple 45. Si $n = 3$ et $t = 1003$, l'équation définissant E est

$$E\colon y^2 = x^3 + 1003x^2 - 9720x + 729.$$

Le point $(0, 27)$ est non-divisible par le théorème 44. À l'aide de la fonction `ellrank` sur PARI/GP, on obtient que E est de rang 2 sur $\mathbb{Q}$ et que $((0, 27), (-153, 4617))$ est un système de générateurs de $E(\mathbb{Q})$.

Exemple 46. Lorsque $n = 5$, et $t = -2527$, E est de la forme

$$E\colon y^2 = x^3 + 2527x^2 - 65050x + 15625.$$

Par le théorème 44, le point $(0, 125)$ est non-divisible. De plus à l'aide de PARI/GP, on trouve que E est de rang 1 et sans torsion. On a alors

$$E(\mathbb{Q}) = \langle (0, 125) \rangle.$$

Maintenant, on veut étendre le théorème 44 au cas $|t| < \max(100n^2, n^4)$. On peut utiliser la minoration pour la hauteur établie dans [30, proposition 2.1] : pour tout $P \in E(\mathbb{Q})$ d'ordre infini, si P est non singulier modulo p pour tout nombre premier p, on a

$$\widehat{h}(P) > \frac{1}{12N^2} \log |\Delta_{\min}|,$$

où N est le nombre défini dans [30, théorème 1] et $\Delta_{\min}$ est le discriminant minimal E. Soit C_E le plus petit multiple commun des nombres de Tamagawa de E et soit $P \in E(\mathbb{Q})$ un point d'ordre infini. Le point $C_E P$ est non singulier modulo p pour tout nombre premier p et donc on a

$$\widehat{h}(P) > \frac{1}{12N^2 C_E^2} \log |\Delta_{\min}|.$$

Puisque $\Delta > 0$, on a $N = 6$ ou $N = 8$. Ainsi, on obtient pour tout $P \in E(\mathbb{Q})$ d'ordre infini

$$\widehat{h}(P) > \frac{1}{768C_E^2} \log |\Delta_{\min}|. \tag{1.13}$$

Notons B_E cette minoration. Donc pour un t donné, il suffit de vérifier que $(0, n^3)$ est différent ℓP pour tout $P \in E(\mathbb{Q})$ et tout nombre premier $\ell \leq \sqrt{\dfrac{\widehat{h}(0,n^3)}{B_E}}$.

On utilise la méthode suivante : s'il existe un nombre premier ℓ et un point $P \in E(\mathbb{Q})$ tel que $\ell P = (0, n^3)$ alors pour tout nombre premier $p \nmid \Delta$, comme la réduction de E modulo p est une courbe elliptique sur $\mathbb{F}_p$, $\ell\overline{P} = \overline{(0, n^3)}$, où $\overline{P}$ est la réduction modulo p de P. Puisque $p \nmid \Delta$ et que le point P est entier, la réduction modulo p de P est bien définie et définit un point de $E(\mathbb{F}_p)$. Si p est un nombre premier tel que ℓ divise l'exposant du groupe $E(\mathbb{F}_p)$ noté r_p, on doit avoir $\dfrac{r_p}{\ell}\overline{(0, n^3)} = O$. Ainsi, si on trouve un nombre premier p tel que $\ell \mid r_p$ et $\frac{r_p}{\ell}\overline{(0, n^3)} \neq O$, il n'existe pas de point $P \in E(\mathbb{Q})$ tel que $\ell P = (0, n^3)$. Cette méthode permet d'établir un algorithme qui teste si $\frac{r_p}{\ell}\overline{(0, n^3)} = O$ pour un grand nombre de nombres premiers p et qui s'arrête dès qu'un nombre premier p tel que $\frac{r_p}{\ell}\overline{(0, n^3)} \neq O$ est découvert. Cet algorithme est implémenté dans la fonction `divisible_locale` (voir annexe A.1), et la fonction `test_div` qui exécute la fonction `divisible_locale` sur tous les entiers $\ell \leq \sqrt{\dfrac{\widehat{h}(0,n^3)}{B_E}}$.

On obtient le résultat suivant.

Théorème 47. *Si $n \leq 15$ et δ est sans facteurs carrés, alors le point $(0, n^3)$ n'est pas divisible.*

Démonstration. Pour $n = 1$, le théorème 44 implique que si $|t| \geq 100$, alors le point $(0, 1)$ n'est pas divisible. On remarque également que le résultat est vrai pour des valeurs de t strictement négatives car $(0, 1)$ est le seul point entier appartenant à $E(\mathbb{Q}) - E_0(\mathbb{Q})$. Pour $1 \leq t < 100$, il suffit d'utiliser la méthode décrite précédemment à l'aide de PARI/GP. Pour $2 \leq n \leq 15$, on utilise une méthode similaire. □

Exemple 48. Pour $n = 11$, $t = 4$, ici $\delta = 133237 = 13 \times 37 \times 277$ est sans facteurs carrés. Par le théorème 47, le point $(0, 1331) \in E(\mathbb{Q})$ est non-divisible.

Chapitre 2

Paramétrisation modulaire sur les corps de fonctions

Soit q une puissance d'un nombre premier p et E une courbe elliptique définie sur $\mathbb{F}_q(T)$ par le modèle de Weierstrass

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{F}_q[T].$$

On suppose que E est non-isotriviale et qu'elle est de mauvaise réduction multiplicative totalement déployée en la place $\infty = 1/T$. Par les travaux de Drinfeld, Grothendieck, Jacquet et Langlands ([15, 29]), il existe une "paramétrisation modulaire" $\Phi\colon \overline{M}_{\Gamma_0(n)} \to E$, où n est la partie finie du conducteur de E, et $\overline{M}_{\Gamma_0(n)}$ est la courbe modulaire de Drinfeld sur $\mathbb{F}_q(T)$ associée au sous-groupe de congruence de Hecke $\Gamma_0(n)$. L'application Φ a été étudiée et décrite par différents auteurs, en particulier Gekeler-Reversat [26] et Gekeler [20, 22]. Nous allons décrire une méthode pour calculer *exactement* les images $\Phi(c) \in E$ des pointes $c \in \overline{M}_{\Gamma_0(n)}$.

La situation doit être comparée avec le cas classique en caractéristique zéro. Dans ce cas, si F est une courbe elliptique définie sur $\mathbb{Q}$ de conducteur N, par une série de travaux culminant avec [47, 4], il existe une paramétrisation modulaire donnée par la composée $\varphi\colon X_0(N) \stackrel{\phi}{\to} \mathbb{C}/\Lambda \stackrel{\wp}{\to} F(\mathbb{C})$, où Λ est le réseau des périodes de F, l'application ϕ s'exprime à l'aide de la forme modulaire f de poids 2 associée à F, et l'isomorphisme $\wp$ est donné par la fonction de Weierstrass et sa dérivée. Dans la littérature on trouve de nombreuses études sur la description explicite de ϕ et le calcul de ses invariants arithmétiques : son degré ([55, 10, 12, 51]), ses points critiques ([32, 7, 13]), son évaluation en les pointes ([5, 54]), ses évaluations explicites en les points de Heegner ([52]).

Dans la situation des courbes modulaires de Drinfeld, le fait que E possède une réduction multiplicative déployée en ∞ implique l'existence d'un paramètre de Tate $t \in \mathbb{C}_\infty^*$ et d'un isomorphisme $E(\mathbb{C}_\infty) \simeq \mathbb{C}_\infty^*/t^{\mathbb{Z}}$ où $\mathbb{C}_\infty$ est un complété d'une clôture algébrique de $\mathbb{F}_q((1/T))$. D'une part, la paramétrisation modulaire est donnée de la même manière que dans le cas classique par une application

$$\Phi\colon \overline{M}_{\Gamma_0(n)} \to \mathbb{C}_\infty^*/t^{\mathbb{Z}}$$

où Φ sera définie dans la section 2.6. D'autre part, à l'inverse du cas classique, le degré Φ se calcule très facilement avec la formule de Gekeler [20] rappelée dans le théorème 98. La définition de Φ nécessite également de nombreux outils théoriques que nous allons rappeler tout au long de ce chapitre. À noter qu'un algorithme pour le calcul de cette paramétrisation modulaire est décrit par Bermudez Tobon dans [2] en définissant les fonctions thêta à l'aide d'intégrales. Dans notre approche, nous restons avec la définition des fonctions thêta en termes de produits.

Ce travail a donné lieu à un travail disponible sur Arxiv ([35]). Ce chapitre en est une version plus détaillée.

On garde les même notations que dans l'introduction (voir page 13).

2.1 Arbre de Bruhat-Tits

Pour cette section, les références principalement utilisées sont [26], [20] et [25].

2.1.1 Définition, premières propriétés

On rappelle que $O_\infty = \{x \in K_\infty, |x| \leq 1\}$ est l'anneau des entiers de K_∞ et que $\pi = \frac{1}{T}$ est une uniformisante de K_∞. Un O_∞-réseau est un O_∞-module de K_∞^2 libre de rang 2. On dit que deux réseaux L et L' sont équivalents s'il existe $x \in K_\infty^*$ tel que $L' = xL$. La relation ainsi définie est une relation d'équivalence. On note $[L]$ la classe d'équivalence d'un réseau L.

Définition 49. *L'*arbre de Bruhat-Tits $\mathcal{T}$ *est le graphe combinatoire ayant pour ensemble de sommets $X(\mathcal{T})$ l'ensemble des classes $[L]$ de réseaux de K_∞^2 et pour ensemble d'arêtes orientées $Y(\mathcal{T})$ l'ensemble des couples $([L],[L'])$ tels qu'il existe $L_1 \in [L], L_2 \in [L']$ vérifiant $\pi L_1 \subsetneq L_2 \subsetneq L_1$.*

À noter que la condition $\pi L_1 \subsetneq L_2 \subsetneq L_1$ est équivalente à $\dim_{\mathbb{F}_q} L_1/L_2 = 1$. Le graphe $\mathcal{T}$ est muni de deux applications naturelles $o, t\colon Y(\mathcal{T}) \to X(\mathcal{T})$

définies par : pour $e = ([L], [L']) \in Y(\mathcal{T})$, $o(e) = [L]$ et $t(e) = [L']$. Pour une arête $e = ([L], [L']) \in Y(\mathcal{T})$ on note $\overline{e}$ l'arête opposée $([L'], [L])$.
Le graphe $\mathcal{T}$ est un arbre au sens de Serre (voir [39, I.2]) c'est-à-dire un graphe infini sans circuit. En particulier deux sommets de $\mathcal{T}$ sont reliés par une unique géodésique. L'arbre $\mathcal{T}$ est $(q+1)$-régulier, c'est-à-dire de chaque sommet partent $q+1$ arêtes. En effet, pour $v = [L] \in X(\mathcal{T})$, si l'on note p_L la projection canonique $L \to L/\pi L$, on a la bijection suivante

$$\begin{array}{ccc} \mathbb{P}^1(L/\pi L) & \xrightarrow{\sim} & \{w \in X(\mathcal{T}),\ w \text{ voisin de } v\} \\ \ell & \mapsto & [p_L^{-1}(\ell)]. \end{array}$$

On note $\mathcal{Z}$ le centre de $\mathrm{Gl}_2(K_\infty)$ et $\mathcal{I}_\infty$ le sous-groupe d'Iwahori défini par

$$\mathcal{I}_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(O_\infty), c \equiv 0\ [\pi] \right\}.$$

Le groupe $\mathrm{Gl}_2(K_\infty)$ agit naturellement à gauche sur l'ensemble des réseaux de K_∞^2 de la manière suivante :

$$g * [L] = [gL], \qquad (g \in \mathrm{Gl}_2(K_\infty), [L] \in X(\mathcal{T}))\,.$$

Comme l'action de $\mathrm{Gl}_2(K_\infty)$ est transitive et le stabilisateur de l'élément $[O_\infty \oplus O_\infty]$ est $\mathcal{Z}\,\mathrm{Gl}_2(O_\infty)$, on obtient l'identification suivante :

$$\begin{array}{ccc} \mathrm{Gl}_2(K_\infty)/\mathcal{Z}\,\mathrm{Gl}_2(O_\infty) & \to & X(\mathcal{T}) \\ g \mod \mathcal{Z}\,\mathrm{Gl}_2(O_\infty) & \mapsto & [g(O_\infty \oplus O_\infty)]. \end{array} \tag{2.1}$$

De plus, les sommets $[O_\infty \oplus O_\infty]$ et $[\pi^{-1}O_\infty \oplus O_\infty]$ étant voisins et puisque le stabilisateur de $[\pi^{-1}O_\infty \oplus O_\infty]$ est $\mathcal{Z}\mathcal{I}_\infty \subset \mathcal{Z}\,\mathrm{Gl}_2(O_\infty)$, on obtient l'identification suivante pour $Y(\mathcal{T})$:

$$\begin{array}{ccc} \mathrm{Gl}_2(K_\infty)/\mathcal{Z}\mathcal{I}_\infty & \to & Y(\mathcal{T}) \\ g \mod \mathcal{Z}\mathcal{I}_\infty & \mapsto & ([g(O_\infty \oplus O_\infty)], [g(\pi^{-1}O_\infty \oplus O_\infty)])\,. \end{array} \tag{2.2}$$

Si une arête $e \in Y(\mathcal{T})$ correspond via l'identification précédente à la classe d'une matrice $g \in \mathrm{Gl}_2(K_\infty)$, alors l'arête opposée $\overline{e}$ correspond à la classe de la matrice $g\varpi$, où $\varpi = \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}$. On considère l'ensemble

$$\mathcal{H} = \left\{ \begin{pmatrix} u & 1 \\ 1 & 0 \end{pmatrix},\ u \in \mathbb{F}_q^* \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \tag{2.3}$$

L'ensemble $\mathcal{H}$ forme un système de représentants de $\mathrm{Gl}_2(O_\infty)/\mathcal{I}_\infty$. Les identifications (2.1) et (2.2) permettent de déterminer l'ensemble des sommets voisins de n'importe quel sommet de $\mathcal{T}$. En effet, si $v \in X(\mathcal{T})$ représenté par $g \in \mathrm{Gl}_2(K_\infty)$, l'ensemble des arêtes d'origine v peut être représenté par l'ensemble des matrices $(gh)_{h\in\mathcal{H}} \subset \mathrm{Gl}_2(K_\infty)$. Ainsi les sommets voisins de v sont représentés par les matrices $(gh\varpi)_{h\in\mathcal{H}} \subset \mathrm{Gl}_2(K_\infty)$.
Une demi-droite de $\mathcal{T}$ est un sous-graphe de $\mathcal{T}$ de la forme $\bullet-\bullet-\bullet-\cdots$. On dit que deux demi-droites sont *équivalentes* si et seulement si elles diffèrent d'un graphe fini. Un *bout* (ou une *fin*) de $\mathcal{T}$ est une classe d'équivalence de demi-droites. On note $\mathcal{F}(\mathcal{T})$ l'ensemble des bouts de $\mathcal{T}$.

Proposition 50. *Il existe une bijection canonique* $\Psi\colon \mathcal{F}(\mathcal{T}) \to \mathbb{P}^1(K_\infty)$.

Démonstration. Soit s un bout de $\mathcal{T}$. On choisit une demi-droite la représentant :

$$([L_0], [L_1], \ldots).$$

On peut choisir les réseaux $(L_i)_{i\geq 0}$ de telle sorte que pour tout $i \geq 0$: $L_{i+1} \subset L_i$ et $L_i \not\subset \pi L_0$. Ainsi le O_∞-module engendré par $(\cap_{i\geq 0} L_i)$ est de rang au plus 1. Pour tout $i \geq 0$, il existe une O_∞-base (x_i, y_i) de L_0 telle que L_i soit engendré par $\pi^i x_i$ et y_i. On a alors $y_{i+1} = a_i\pi^i x_i + y_i$, et $y_{i+1} - y_i \in \pi^i L_0$ avec $a_i \in O_\infty$. Ainsi la suite $(y_i)_{i\geq 0}$ est de Cauchy dans K_∞^2 donc convergente et dont la limite est élément non nul $y \in \cap_{i\geq 0} L_i$.
On construit ainsi une application $\Psi\colon \mathcal{F}(\mathcal{T}) \to \mathbb{P}^1(K)$ en associant à une demi-droite $([L_i])_{i\geq 0}$ la droite engendrée par $\cap_{i\geq 0} L_i$. L'application Ψ ainsi construite est surjective. En effet, si $x \in K_\infty^2 - \{0\}$, il suffit de prendre la demi-droite $([L_i])_{i\geq 0}$, où $L_i = O_\infty x \oplus O_\infty \pi^i y$, où $y \in K_\infty^2$ est un vecteur de K_∞^2 quelconque linéairement indépendant de x.
Pour l'injectivité, soient $([L_i])_{i\geq 0}$ et $([L'_i])_{i\geq 0}$ tels que $\cap_{i\geq 0} L_i$ et $\cap_{i\geq 0} L'_i$ engendrent la même droite dans K_∞^2. Quitte à multiplier par un scalaire, on peut supposer $\cap_{i\geq 0} L_i = \cap_{i\geq 0} L'_i = O_\infty x$, avec $x \in K_\infty^2$. On élimine si nécessaire les premiers termes des suites $(L_i)_{i\geq 0}$ et $(L'_i)_{i\geq 0}$, et on peut supposer que $L_0 = O_\infty x \oplus O_\infty y$, et que $L'_0 = O_\infty x \oplus O_\infty y'$ avec y, y' deux vecteurs de K_∞^2 convenables. Du fait que pour tout $i \geq 0$, $x \in L_i$ et $\#L_0/L_i = q^i$, on a $L_i = O_\infty x \oplus O_\infty \pi^i y$. Par un argument similaire, on a que L'_i est engendré par x et $\pi^i y'$. Puisque l'on a $\pi^n y' = ax + by$, où $a, b \in O_\infty$, et que n est un entier suffisamment grand, on obtient que L'_{n+i} est engendré par x et $\pi^i by$ et donc coïncide avec un réseau L_{i+j} avec $j \geq 0$. On en conclut que les deux demi-droites portées par les sommets $([L_i])_{i\geq 0}$ et $([L'_i])_{i\geq 0}$ ne diffèrent que d'un graphe fini et sont donc équivalentes. □

Pour $n \in \mathbb{Z}$, on note v_n le sommet correspondant à la classe $[O_\infty \oplus \pi^n O_\infty]$. Le sommet v_n correspond par l'identification (2.1) à la classe de la matrice

$\begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix}$. Le bout constitué des sommets $(v_n)_{n\geq 0}$ correspond via la bijection Ψ au point $\infty = [1,0] \in \mathbb{P}^1(K_\infty)$.

Définition 51. *Soient $s \in \mathcal{F}(\mathcal{T})$ un bout et $e \in Y(\mathcal{T})$ une arête. Puisque $\mathcal{T}$ est un arbre, il existe une unique demi-droite $\mathcal{D}$ représentant s donnée par des sommets $(\nu_k)_{k\in\mathbb{N}}$ telle que $\nu_0 = o(e)$. On dit alors que e* pointe vers *s si $e \in \mathcal{D}$.*

Le bout ∞ permet de définir une orientation sur $\mathcal{T}$. On dit qu'une arête e est *orientée positivement* si e pointe vers ∞, dans le cas contraire on dit que e est *orientée négativement*. On notera $Y^+(\mathcal{T})$ (respectivement $Y^-(\mathcal{T})$) l'ensemble des arêtes orientées positivement (respectivement négativement).

Dans toute la suite, on considère l'arbre de Bruhat-Tits en terme d'espaces quotients de $\mathrm{Gl}_2(K_\infty)$ provenant des identifications (2.1) et (2.2).

Lemme 52.

1. *L'ensemble $\left\{ \begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z}, y \in K_\infty/\pi^n O_\infty \right\}$ forme un système de représentants de $X(\mathcal{T})$ et de $Y^+(\mathcal{T})$.*
2. *L'ensemble $\left\{ \begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix} \varpi, n \in \mathbb{Z}, y \in K_\infty/\pi^n O_\infty \right\}$ forme un système de représentants pour $Y^-(\mathcal{T})$.*

Démonstration. On peut trouver cette preuve dans [6, lemme 2.7]. Cette algorithme de réduction est utile dans la suite, on choisit donc d'en présenter la démonstration. Soit $B = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathrm{Gl}_2(K_\infty)$. Quitte à multiplier par la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Gl}_2(O_\infty)$, on peut supposer $v_\infty(x_3) \geq v_\infty(x_4)$. La multiplication à droite de B par la matrice $\begin{pmatrix} x_4^{-1} & 0 \\ -x_3 x_4^{-2} & x_4^{-1} \end{pmatrix} \in \mathcal{Z}\mathrm{Gl}_2(O_\infty)$ nous donne

$$\begin{pmatrix} x_1 x_4^{-1} - x_2 x_3 x_4^{-2} & x_2 x_4^{-1} \\ 0 & 1 \end{pmatrix} \in \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \mathcal{Z}\mathrm{Gl}_2(O_\infty),$$

donc une matrice de la forme

$$\begin{pmatrix} y_1 & y_2 \\ 0 & 1 \end{pmatrix}$$

avec $y_1, y_2 \in K_\infty$. Soit $n = v_\infty(y_1)$. Écrivons $y_1 = \pi^n \epsilon$ avec $\epsilon \in O_\infty^*$. La multiplication de $\begin{pmatrix} y_1 & y_2 \\ 0 & 1 \end{pmatrix}$ à droite par $\begin{pmatrix} \epsilon^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ nous donne une matrice

de la forme $\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}$.

Soient $B = \begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} \pi^m & z \\ 0 & 1 \end{pmatrix}$ avec $m, n \in \mathbb{Z}$, $y \in K_\infty/\pi^n O_\infty$ et $z \in K_\infty/\pi^m O_\infty$. On suppose que B et C sont équivalentes modulo $\mathcal{Z}\mathrm{Gl}_2(O_\infty)$. Il existe donc $\begin{pmatrix} u & r \\ s & t \end{pmatrix} \in \mathrm{Gl}_2(O_\infty)\mathcal{Z}$ telle que

$$\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pi^m & z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & r \\ s & t \end{pmatrix} = \begin{pmatrix} \pi^m u + zs & \pi^m r + zt \\ s & t \end{pmatrix}.$$

On a alors $s = 0$ et $t = 1$. Il vient donc $r \in O_\infty^*$ et donc que $n = m$. Puis on obtient $y = z + \pi^n$ donc $y \equiv z\ [\pi^n]$.
Pour une arête $e \in Y(\mathcal{T})$, on note $v = o(e)$ son sommet de départ. Par ce qu'on a montré précédemment le sommet v peut être représenté par une matrice B de la forme $\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}$, avec $n \in \mathbb{Z}$ et $y \in K_\infty/\pi^n O_\infty$. Les arêtes d'origine v peuvent alors s'écrire sous la forme Bh, avec $h \in \mathcal{H}$. Il suffit de remarquer que l'unique arête e orientée positivement partant de v est de la forme Bh avec $h = I_2$. Cela montre le résultat pour $Y^+(\mathcal{T})$.

Pour $Y^-(\mathcal{T})$, il suffit de remarquer que si $e \in Y^-(\mathcal{T})$ alors $e = \overline{e}\varpi$ et que $\overline{e} \in Y^+(\mathcal{T})$. □

Pour $n \in \mathbb{Z}$, $y \in K_\infty/\pi^n O_\infty$ on note $v(n, y)$ (respectivement $[n, y]$) le sommet (respectivement l'arête orientée positivement) représenté par la matrice $\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}$. Si $e \in Y(\mathcal{T})$ est orientée négativement et $\overline{e} = [n, y]$ avec $n \in \mathbb{Z}$ et $y \in K_\infty/\pi^n O_\infty$, on note $e = [n, y]\varpi$. Avec cette notation le sommet v_n correspond à $v(-n, 0)$, et on note e_n l'arête reliant v_n à v_{n+1}.

Soit $\Gamma \subset \mathrm{Gl}_2(A)$ un sous-groupe arithmétique. Le groupe Γ agit sur $\mathcal{T}$ par multiplication à gauche. L'action de Γ est sans inversion. Ainsi le graphe quotient $\Gamma\backslash\mathcal{T}$ existe comme étant le graphe ayant pour ensemble de sommets $X(\Gamma\backslash\mathcal{T}) = \Gamma\backslash X(\mathcal{T})$ et pour ensemble d'arêtes $Y(\Gamma\backslash\mathcal{T}) = \Gamma\backslash Y(\mathcal{T})$. On note G_n le stabilisateur de v_n sous l'action de $\mathrm{Gl}_2(A)$. On a

$$G_0 = \mathrm{Gl}_2(\mathbb{F}_q)$$
$$G_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(A),\ \deg(b) \leq n \right\} \qquad (n \geq 1).$$

Le stabilisateur de e_k est $G_k \cap G_{k+1}$. Pour $v \in X(\mathcal{T})$ (respectivement $e \in Y(\mathcal{T})$), on note $\tilde{v}$ (respectivement $\tilde{e}$) la classe de v (respectivement e) modulo Γ.

Proposition 53. *[53, page 212] Pour $\Gamma = \mathrm{Gl}_2(A)$, le graphe quotient $\Gamma\backslash\mathcal{T}$ est une demi-droite représentée par les sommets $(v_k)_{k\in\mathbb{N}}$ et les arêtes $(e_k)_{k\in\mathbb{N}}$. Autrement dit, $\Gamma\backslash\mathcal{T}$ est de la forme*

$$\overset{v_0}{\bullet} \overset{e_0}{\to} \overset{v_1}{\bullet} \overset{e_1}{\to} \overset{v_2}{\bullet} \overset{e_2}{\to} ....$$

Démonstration. Pour $A, B \in \mathrm{Gl}_2(K_\infty)$ on notera $A \sim B$ si $A \in B\mathcal{Z}\,\mathrm{Gl}_2(O_\infty)$. Pour deux sommets $v, v' \in X(\mathcal{T})$, on notera $v \approx v'$ si $v' = \gamma v$ avec $\gamma \in \mathrm{Gl}_2(A)$. Soit $v \in X(\mathcal{T})$. Par le lemme 52, v admet un représentant de la forme $\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}$, avec $n \in \mathbb{Z}$ et $y \in K_\infty \mod (\pi^n O_\infty)$. On écrit $y = P + y_0$, avec $P \in A$ et $y_0 \in K_\infty$ vérifiant $0 < v_\infty(y_0) < n$ si $y_0 \neq 0$ et $y_0 = 0$ sinon. Premier cas : si $n \leq 0$ alors $y_0 = 0$, et on a

$$\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix} \approx \begin{pmatrix} \pi^n & 0 \\ 0 & 1 \end{pmatrix}.$$

Second cas : si $n > 0$, on a

$$\begin{aligned}
\begin{pmatrix} \pi^n & 0 \\ 0 & 1 \end{pmatrix} &\approx \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \pi^n & 0 \\ 0 & 1 \end{pmatrix} \\
&\sim \begin{pmatrix} 0 & 1 \\ -\pi^n & y_0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \pi^n y_0^{-1} & 1 \end{pmatrix} \\
&\sim \begin{pmatrix} -\pi^n y_0^{-1} & 1 \\ 0 & y_0 \end{pmatrix} \begin{pmatrix} y_0^{-1} & 0 \\ 0 & y_0^{-1} \end{pmatrix} \\
&\sim \begin{pmatrix} -\pi^n y_0^{-2} & y_0^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -y_0^2 \pi^{-2} v_\infty(y_0) & 0 \\ 0 & 1 \end{pmatrix} \\
&\sim \begin{pmatrix} \pi^{n-2v_\infty(y_0)} & y_0^{-1} \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

On décompose y_0^{-1} sous la forme $y_0^{-1} = y_1 + Q$ avec $Q \in A$ et $y_1 \in K_\infty$ vérifiant $y_1 = 0$ ou $0 \leq v_\infty(y_1) < n - 2v_\infty(y_0)$. Si $n - 2v_\infty(y_0) \leq 0$, on est ramené au premier cas. Si $n - 2v_\infty(y_0) > 0$ on est ramené au second cas. On réitère le processus jusqu'à son aboutissement. □

Définition 54. *Un sommet $v \in X(\mathcal{T})$ (respectivement une arête $e \in Y(\mathcal{T})$ est dit de* type k*, et on notera* $\mathrm{type}(v) = k$ *si son image dans $\mathrm{Gl}_2(A)\backslash\mathcal{T}$ est v_k (respectivement e_k).*

La preuve de la proposition 53 donne un algorithme qui à un sommet $v \in X(\mathcal{T})$ donné sous la forme $v = v(n, y)$ avec $n \in \mathbb{Z}$ et $y \in K_\infty/\pi^n O_\infty$ renvoie son type k et une matrice $\gamma \in \mathrm{Gl}_2(A)$ telle que $v = \gamma v_k$ (voir la fonction `Returnmat` dans l'annexe A.2).

2.1.2 Graphe quotient $\Gamma\backslash\mathcal{T}$

Dans toute cette partie on considère $\Gamma = \Gamma_0(n)$ avec $n \in A$, unitaire et non constant et on pose $d = \deg(n)$. Grâce aux travaux de Serre ([39, II 1.2, II 1.3]), on sait que le graphe quotient $\Gamma\backslash\mathcal{T}$ est une union disjointe de la forme

$$(\Gamma\backslash\mathcal{T})^0 \cup (\cup h_i)$$

où $(\Gamma\backslash\mathcal{T})^0$ est un graphe fini connexe et les h_i sont des demi-droites appelées *pointes* de $\Gamma\backslash\mathcal{T}$. Les pointes de $\Gamma\backslash\mathcal{T}$ sont en nombre fini, et en particulier on a

Lemme 55. *[49, Lecture 12, Théorème 4.3] Les ensembles suivants sont en bijection canonique :*

1. *les pointes de* $\Gamma\backslash\mathcal{T}$ *;*
2. *les pointes de la courbe modulaire* $\overline{M}_\Gamma$ *;*
3. *l'ensemble des orbites* $\Gamma\backslash\mathbb{P}^1(K)$.

L'objectif de cette partie est de rappeler une méthode déterminée par Gekeler-Nonnengardt dans [25] permettant de calculer le graphe quotient en identifiant des sous-ensembles du graphe $\Gamma\backslash\mathcal{T}$ et plus particulièrement le graphe fini $(\Gamma\backslash\mathcal{T})^0$ avec des espaces quotients de l'espace projectif sur A/n. Pour $v \in X(\mathcal{T})$, on notera $\tilde{v}$ la classe de v dans $\Gamma\backslash\mathcal{T}$. On définit pour tout $i \in \mathbb{N}$, les ensembles

$$X_i(\Gamma\backslash\mathcal{T}) = \{\tilde{v} \in X(\Gamma\backslash\mathcal{T}), \mathrm{type}(v) = i\},$$
$$Y_i(\Gamma\backslash\mathcal{T}) = \{\tilde{e} \in Y(\Gamma\backslash\mathcal{T}), \mathrm{type}(e) = i\}.$$

À noter que $\mathrm{type}(v)$ ne dépend que de la classe $\tilde{v}$ de v.

Lemme 56. *[25, 1.6] On a les bijections suivantes :*

$$\begin{array}{rcl} G_i\backslash\,\mathrm{Gl}_2(A)/\Gamma & \to & X_i(\Gamma\backslash\mathcal{T}) \\ \overline{\gamma} & \mapsto & \widetilde{\gamma^{-1}v_i} \end{array} \tag{2.4}$$

$$\begin{array}{rcl} (G_i \cap G_{i+1})\backslash\,\mathrm{Gl}_2(A)/\Gamma & \to & Y_i(\Gamma\backslash\mathcal{T}) \\ \overline{\gamma} & \mapsto & \widetilde{\gamma^{-1}e_i}. \end{array} \tag{2.5}$$

La conséquence du dernier lemme est que l'on peut identifier les sommets (respectivement les arêtes) de type i du graphe $\Gamma\backslash\mathcal{T}$ avec les orbites de $\mathrm{Gl}_2(A)/\Gamma$ sous l'action de G_i (respectivement $G_i \cap G_{i+1}$).

Soit

$$\mathbb{P}^1(A/n) = \{[u,v], u, v \in A/n, u(A/n) + v(A/n) = A/n\},$$

où $[u,v]$ est la classe d'équivalence de (u,v) modulo $(A/n)^\times$. Sur $\mathbb{P}^1(A/n)$, on peut faire agir $\mathrm{Gl}_2(A)$ de la manière suivante :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} [u,v] = [au+bv, cu+dv].$$

On a la bijection suivante

$$\begin{array}{ccc} \mathrm{Gl}_2(A)/\Gamma & \xrightarrow{\sim} & \mathbb{P}^1(A/n) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & [a,c] \end{array} \tag{2.6}$$

qui permet les identifications :

$$\begin{array}{ccc} G_i\backslash\mathbb{P}^1(A/n) & \xrightarrow{\sim} & X_i(\Gamma\backslash\mathcal{T}) \\ [a,c] \mod G_i & \mapsto & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} v_i, \end{array} \tag{2.7}$$

$$\begin{array}{ccc} (G_i \cap G_{i+1})\backslash\mathbb{P}^1(A/n) & \xrightarrow{\sim} & Y_i(\Gamma\backslash\mathcal{T}) \\ [a,c] \mod G_i \cap G_{i+1} & \mapsto & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} v_i. \end{array} \tag{2.8}$$

Cette identification permet de déterminer sommets et arêtes de type i dans $\Gamma\backslash\mathcal{T}$, pour tout $i \in \mathbb{N}$.

Lemme 57. *[25, 1.8] Le sous-graphe de $\Gamma\backslash\mathcal{T}$ constitué des arêtes de type supérieur ou égal à $d-1$ est une union disjointe de demi-droites contenues dans l'ensemble des pointes de $\Gamma\backslash\mathcal{T}$. Autrement dit, les arêtes $e \in Y(\Gamma\backslash\mathcal{T})$ vérifiant $\mathrm{type}(e) \geq d-1$ sont situées sur les pointes de $\Gamma\backslash\mathcal{T}$.*

Une conséquence du lemme est qu'il suffit de déterminer les sommets de type inférieur ou égal à $d-1$ et les arêtes de type inférieur strict à $d-1$ pour déterminer $(\Gamma\backslash\mathcal{T})^0$.

Lemme 58. *[25, 1.11] Soit $v, v' \in X(\mathcal{T})$ deux sommets tels que $\mathrm{type}(v) = \mathrm{type}(v') = r$. Soient $\gamma, \gamma' \in \mathrm{Gl}_2(A)$ deux matrices telles que $v = \gamma v_r$ et $v' = \gamma' v_r$. Alors il existe $\alpha \in \Gamma_0(n)$ telle que $v = \alpha v'$ si et seulement si $\gamma' G_r \gamma^{-1} \cap \Gamma_0(n) \neq \emptyset$.*

Le lemme précédent donne une condition nécessaire et suffisante pour que deux sommets soient équivalents modulo $\Gamma_0(n)$. De plus, pour deux sommets $v, v' \in X(\mathcal{T})$ il permet de déterminer l'ensemble fini des éléments $\gamma \in \Gamma_0(n)$ tels que $v' = \gamma v$.

Exemple 59. On se place sur $A = \mathbb{F}_2[T]$, $n = T^3$. Cet exemple a déjà été traité par différents auteurs dans la littérature notamment Gekeler dans [17]. Puisque $\deg(n) = 3$, il suffit de déterminer les arêtes de type inférieur strictement à 2 et les sommets de type inférieur ou égale à 2. Dans le tableau suivant $\mathcal{R}$ représente un système de représentants de $G_0\backslash\mathbb{P}^1(A/n)$, $\#\omega$ représente le cardinal de l'orbite sous l'action de G_0 d'un point de $\mathbb{P}^1(A/n)$.

Notation	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{00}$	$[1,0]$	3	$v(1,0)$
$\tilde{v}_{01}$	$[T,1]$	6	$v(2,\pi)$
$\tilde{v}_{02}$	$[T^2,1]$	3	$v(4,\pi^2)$

TABLE 2.1 – Sommets de type 0

Les arêtes de type 0 de sommet d'origine $\tilde{v}$ s'identifient aux orbites de la restriction de l'action à $(G_0 \cap G_1)$ sur l'ensemble $G_0[u,v]$, où $[u,v]$ est l'élément identifié à $\tilde{v}$ via la bijection 2.7. Dans le tableau suivant $\mathcal{R}$ représente un système de représentants de $(G_0 \cap G_1)\backslash\mathbb{P}^1(A/n)$.

Notation	$\mathcal{R}$	$\#\omega$	$o(\tilde{e})$	Représentant dans $Y(\mathcal{T})$
$\tilde{e}_{00}$	$[1,0]$	1	$\tilde{v}_{00}$	$[0,0]$
$\tilde{e}_{01}$	$[0,1]$	2	$\tilde{v}_{00}$	$[-1,0]\varpi$
$\tilde{e}_{02}$	$[T,1]$	2	$\tilde{v}_{01}$	$[2,\pi]$
$\tilde{e}_{03}$	$[1,T]$	2	$\tilde{v}_{01}$	$[3,\pi]\varpi$
$\tilde{e}_{04}$	$[T^2+T+1,1]$	2	$\tilde{v}_{01}$	$[2,\pi]\varpi$
$\tilde{e}_{05}$	$[T^2,1]$	2	$\tilde{v}_{02}$	$[4,\pi^2]$
$\tilde{e}_{06}$	$[1,T^2]$	2	$\tilde{v}_{02}$	$[5,\pi^2]\varpi$

TABLE 2.2 – Décomposition en arêtes de type 0

Dans le tableau suivant, $\mathcal{R}$ représente un système de représentants de $G_1\backslash\mathbb{P}^1(A/n)$.

Notation	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{10}$	$[1,0]$	1	$v(-1,0)$
$\tilde{v}_{11}$	$[0,1]$	4	$v(1,0)$
$\tilde{v}_{12}$	$[1,T]$	2	$v(3,\pi)$
$\tilde{v}_{13}$	$[T^2,1]$	4	$v(3,\pi^2)$
$\tilde{v}_{14}$	$[1,T^2]$	1	$v(5,\pi^2)$

TABLE 2.3 – Sommets de type 1

Les arêtes de type 1 s'identifient aux sommets de type 1. En effet, pour tout sommet $\tilde{v} \in X(\Gamma\backslash\mathcal{T})$ de type 1 il existe une unique arête $\tilde{e}$ de type 1 telle que $o(\tilde{e}) = \tilde{v}$. Dans le tableau suivant $\mathcal{R}$ désigne un système de représentants de $G_2\backslash\mathbb{P}^1(A/n)$.

Notation	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{20}$	$[1,0]$	1	$v(-2,0)$
$\tilde{v}_{21}$	$[0,1]$	8	$v(2,0)$
$\tilde{v}_{22}$	$[1,T]$	2	$v(4,\pi)$
$\tilde{v}_{23}$	$[1,T^2]$	1	$v(6,\pi^2)$

TABLE 2.4 – Sommets de type 2

On peut alors déduire la forme du graphe quotient. Dans le dessin suivant les flèches $\dashrightarrow$ désignent les pointes de $\Gamma\backslash\mathcal{T}$.

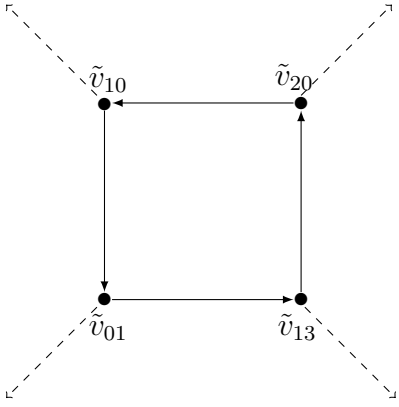


FIGURE 2.1 – Graphe quotient $\Gamma_0(T^3)\backslash\mathcal{T}$ sur $\mathbb{F}_2[T]$

Exemple 60. On se place sur $\mathbb{F}_3[T]$ et un exemple ayant déjà été traité avant par Gekeler dans [17] : $n = T^3 - T^2$. Ici $\deg(n) = 3$, il suffit de déterminer les arêtes de type inférieur strictement à 2 et les sommets de type inférieur ou égal à 2. De nouveau, on note $\mathcal{R}$ un système de représentants de $G_0 \backslash \mathbb{P}^1(A/n)$, et $\#\omega$ représente le cardinal de l'orbite d'un point de $\mathbb{P}^1(A/n)$ sous l'action de G_0.

Notation	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{00}$	$[0:1]$	4	$v(0,0)$
$\tilde{v}_{01}$	$[T:1]$	24	$v(2,\pi)$
$\tilde{v}_{02}$	$[T^2:1]$	12	$v(4,\pi^2)$
$\tilde{v}_{03}$	$[T^2+2T:1]$	8	$v(4,\pi^3+\pi^2)$

TABLE 2.5 – Sommets de type 0

De la même manière que dans l'exemple 59, on regarde la décomposition en arête de type 0. Ici $\mathcal{R}$ représente un système de représentants de $(G_0 \cap G_1) \backslash \mathbb{P}^1(A/n)$.

Notations	$\mathcal{R}$	$\tilde{v} = o(\tilde{e})$	Représentant dans $Y(\mathcal{T})$
$\tilde{e}_{00}$	$[1,0]$	$\tilde{v}_{00}$	$[0,0]$
$\tilde{e}_{01}$	$[0,1]$	$\tilde{v}_{00}$	$[1,0]\varpi$
$\tilde{e}_{02}$	$[T,1]$	$\tilde{v}_{01}$	$[2,\pi]$
$\tilde{e}_{03}$	$[1,T]$	$\tilde{v}_{01}$	$[3,\pi]\varpi$
$\tilde{e}_{04}$	$[2T^2+2T+1,1]$	$\tilde{v}_{01}$	$[3,2\pi^2+\pi]\varpi$
$\tilde{e}_{05}$	$[1,T-1]$	$\tilde{v}_{01}$	$[3,\pi^2+\pi]\varpi$
$\tilde{e}_{06}$	$[T^2,1]$	$\tilde{v}_{02}$	$[4,\pi^2]$
$\tilde{e}_{07}$	$[1,T^2]$	$\tilde{v}_{02}$	$[5,\pi^2]\varpi$
$\tilde{e}_{08}$	$[1,T^2-1]$	$\tilde{v}_{02}$	$[5,\pi^4+2\pi^2+\pi]\varpi$
$\tilde{e}_{09}$	$[T^2+2T,1]$	$\tilde{v}_{03}$	$[4,\pi^3+\pi^2]$
$\tilde{e}_{010}$	$[1,T^2+2T]$	$\tilde{v}_{03}$	$[5,\pi^4+\pi^3+\pi^2]$

TABLE 2.6 – Décomposition en arêtes de type 0

Dans le tableau suivant $\mathcal{R}$ désigne un système de représentants de $G_1 \backslash \mathbb{P}^1(A/n)$.

Notation	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{10}$	$[1:0]$	1	$v(-1,0)$
$\tilde{v}_{11}$	$[0:1]$	9	$v(1,0)$
$\tilde{v}_{12}$	$[1:T]$	6	$v(3,\pi)$
$\tilde{v}_{13}$	$[1:T-1]$	9	$v(3,\pi^2+\pi)$
$\tilde{v}_{14}$	$[T^2:1]$	18	$v(3,\pi^2)$
$\tilde{v}_{15}$	$[1:T^2]$	3	$v(5,\pi^2)$
$\tilde{v}_{16}$	$[1:T^2+2T]$	2	$v(5,\pi^4+\pi^3+\pi^2)$

TABLE 2.7 – Sommets de type 1

De la même manière que dans l'exemple précédent, les arêtes de types 1 dans $\Gamma\backslash\mathcal{T}$ s'identifie au sommets de type 1. Dans le tableau suivant $\mathcal{R}$ désigne un système de représentants de $G_2\backslash\mathbb{P}^1(A/n)$.

Notations	$\mathcal{R}$	$\#\omega$	Représentant dans $X(\mathcal{T})$
$\tilde{v}_{20}$	$[1:0]$	1	$v(-2,0)$
$\tilde{v}_{21}$	$[0:1]$	27	$v(2,0)$
$\tilde{v}_{22}$	$[1:T]$	6	$v(4,\pi)$
$\tilde{v}_{23}$	$[1:T-1]$	9	$v(4,\pi^3+\pi^2+\pi)$
$\tilde{v}_{24}$	$[1:T^2]$	3	$v(6,\pi^2)$
$\tilde{v}_{25}$	$[1:T^2+2T]$	2	$v(6,\pi^5+\pi^4+\pi^3+\pi^2)$

TABLE 2.8 – Sommets de type 2

L'arbre quotient $\Gamma\backslash\mathcal{T}$ est donc de la forme (comme dans l'exemple précédent les flèches $\dashrightarrow$ désignent les pointes de $\Gamma\backslash\mathcal{T}$) :

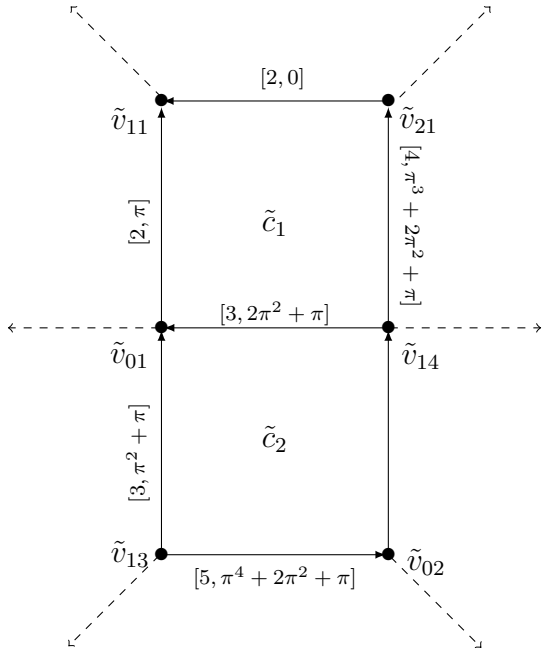


FIGURE 2.2 – Graphe quotient $\Gamma_0(T^3 - T^2)\backslash\mathcal{T}$ sur $\mathbb{F}_3[T]$

2.2 Cochaînes harmoniques

2.2.1 Généralités

Définition 61. *Soit B un groupe abélien. Une application $\varphi\colon Y(\mathcal{T}) \to B$ est appelée* cochaîne harmonique *à valeurs dans B si elle satisfait les conditions suivantes :*

1. *pour tout $e \in Y(\mathcal{T})$, $\varphi(\overline{e}) = -\varphi(e)$,*
2. *pour tout $v \in X(\mathcal{T})$, $\displaystyle\sum_{o(e)=v} \varphi(e) = 0$.*

D'autre part, si pour tout $\gamma \in \Gamma$ et $e \in Y(\mathcal{T})$ on a $\varphi(\gamma e) = \varphi(e)$, on dit que φ est Γ-invariante.

Le groupe additif des cochaînes harmoniques à valeurs dans B est noté $\underline{H}(\mathcal{T}, B)$ et le sous-groupe des cochaînes harmoniques Γ-invariantes est noté $\underline{H}(\mathcal{T}, B)^\Gamma$.

Les éléments de $\underline{H}(\mathcal{T}, B)^\Gamma$ peuvent être considérés comme des applications définies sur les arêtes du graphe quotient $\Gamma\backslash\mathcal{T}$. Soit $v \in X(\mathcal{T})$ un sommet et

$\widetilde{v}$ sa classe d'équivalence modulo Γ. Le stabilisateur de v, noté Γ_v, agit sur l'ensemble

$$\{e \in Y(\mathcal{T}),\ o(e) = v\}.$$

Pour $e \in Y(\mathcal{T})$, soit Γ_e son stabilisateur. La longueur de l'orbite de e est $m(e) = [\Gamma_v : \Gamma_e]$ et ce nombre ne dépend que de la classe $\tilde{e}$ de e dans $\Gamma\backslash\mathcal{T}$. Lorsque l'on regarde $\varphi \in \underline{H}(\mathcal{T}, B)^\Gamma$ comme une application sur $Y(\Gamma\backslash\mathcal{T})$, la condition sur la somme dans la définition 61 devient

$$\sum_{\substack{\tilde{e}\in Y(\Gamma\backslash\mathcal{T}) \\ o(\tilde{e})=\tilde{v}}} m(\tilde{e})\varphi(\tilde{e}) = 0.$$

Définition 62. *Une cochaîne harmonique $\varphi \in \underline{H}(\mathcal{T}, B)^\Gamma$ est dite* parabolique *si elle possède un support fini modulo Γ.*

On note $\underline{H}_!(\mathcal{T}, B)^\Gamma$ le sous-groupe des cochaînes harmoniques paraboliques. Notons que $\underline{H}_!(\mathcal{T}, B)^\Gamma$ est libre si B est libre. On note $\mathbb{Z}[X(\Gamma\backslash\mathcal{T})]$ (respectivement $\mathbb{Z}[Y(\Gamma\backslash\mathcal{T})]$) le groupe libre engendré par les sommets (respectivement arêtes orientées) de $\Gamma\backslash\mathcal{T}$. L'application $e \mapsto (t(e)) - (o(e))$ s'étend linéairement en un morphisme de bord $\partial : \mathbb{Z}[Y(\Gamma\backslash\mathcal{T})] \to \mathbb{Z}[X(\Gamma\backslash\mathcal{T})]$. Le morphisme ∂ passe au quotient en

$$\overline{\partial}\ : \mathbb{Z}[Y(\Gamma\backslash\mathcal{T})]/\mathbb{Z}[(e) + (\overline{e}),\ e \in Y(\Gamma\backslash\mathcal{T})] \to \mathbb{Z}[X(\Gamma\backslash\mathcal{T})].$$

Le premier groupe d'homologie $H_1(\Gamma\backslash\mathcal{T}, \mathbb{Z})$ du graphe $\Gamma\backslash\mathcal{T}$ est le noyau de $\overline{\partial}$.

Proposition 63. *[20, 1.8] Soit $\varphi \in H_1(\Gamma\backslash\mathcal{T}, \mathbb{Z})$. On note $Z(\Gamma)$ le centre de Γ. Pour $e \in \mathcal{T}$, on pose $n(e) := \dfrac{\#\Gamma_e}{\#Z(\Gamma)}$. L'application $\varphi^* : e \mapsto n(e)\varphi(e)$ définit un élément de $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ et l'application $j_\Gamma : \varphi \in H_1(\Gamma\backslash\mathcal{T}, \mathbb{Z}) \mapsto \varphi^* \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ est injective.*

Proposition 64. *[20, 1.8] Le rang g du groupe abélien libre $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ vérifie*

$$g = \mathrm{rg}(H_1(\Gamma\backslash\mathcal{T})) = g(\Gamma),$$

où $g(\Gamma)$ est le genre de la courbe $\overline{M}_\Gamma$.

On va maintenant rappeler une formule pour calculer le genre $g(\Gamma)$ de la courbe modulaire $\overline{M}_\Gamma$ lorsque $\Gamma = \Gamma_0(n)$. Pour $n \in A$, soit $n = \prod_{1\le i\le s} f_i^{r_i}$ la

décomposition en facteurs irréductibles de n. On note $q_i = q^{\deg f_i} = \#A/(f_i)$. On introduit les quantités :

$$\varepsilon(n) = \prod_{1\leq i\leq s} q_i^{r_i-1}(q_i+1),$$
$$\kappa(n) = \prod_{1\leq i\leq s} (q_i^{\lceil \frac{r_i-1}{2}\rceil} + q_i^{\lceil \frac{r_i}{2}\rceil}).$$

Proposition 65. *[25, Théorème 2.17] Le genre de $\Gamma_0(n)$ est donné par*

$$g(\Gamma_0(n)) = 1 + \frac{\varepsilon(n) - (q+1)\kappa(n) - 2^{s-1}\big((r(n)q(q-1) + (q+1)(q-2)\big)}{q^2-1},$$

où $r(n) = 1$ si tous les facteurs irréductibles de n sont de degré pair et 0 sinon.

Corollaire 66. *Si n est irréductible de degré d alors*

$$g(\Gamma_0(n)) = \begin{cases} \dfrac{q^d - q^2}{q^2-1} & \text{si } d \text{ est pair,} \\ \dfrac{q^d - q}{q^2-1} & \text{sinon.} \end{cases}$$

Sur $\underline{H}_!(\mathcal{T},\mathbb{C})^\Gamma$, le produit scalaire de Petersson est défini par

$$\langle \varphi, \psi\rangle = \sum_{\tilde{e}\in Y(\Gamma\backslash\mathcal{T})} \frac{q-1}{2}|\Gamma_e|^{-1}\varphi(\tilde{e})\overline{\psi(\tilde{e})} \qquad (\varphi,\psi\in \underline{H}_!(\mathcal{T},\mathbb{C})^\Gamma). \tag{2.9}$$

Soit $n\in A$. Si $n'\in A$ est un polynôme divisant n alors pour tout diviseur unitaire a de n/n', le plongement $i_{a,n'}\colon \underline{H}_!(\mathcal{T},\mathbb{Q})^{\Gamma_0(n')} \to \underline{H}_!(\mathcal{T},\mathbb{Q})^{\Gamma_0(n)}$ est donné par

$$i_{a,n'}(\varphi)(e) = \varphi\left(\begin{pmatrix} a & 0\\ 0 & 1\end{pmatrix} e\right) \qquad (\varphi\in \underline{H}_!(\mathcal{T},\mathbb{Q})^{\Gamma_0(n')},\ e\in Y(\mathcal{T})).$$

Définition 67. *Soit $\underline{H}_!^{\mathrm{new}}(\mathcal{T},\mathbb{Q})^{\Gamma_0(n)}$ le supplémentaire orthogonal dans $\underline{H}_!(\mathcal{T},\mathbb{Q})$, pour le produit scalaire de Petersson, des images de tous les $i_{a,n'}$ où n' parcourt les diviseurs propres de n et a parcourt les diviseurs propres de n/n'.*
Soit $\underline{H}_!^{\mathrm{new}}(\mathcal{T},\mathbb{Z})^{\Gamma_0(n)} = \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(n)} \cap \underline{H}_!^{\mathrm{new}}(\mathcal{T},\mathbb{Q})^{\Gamma_0(n)}$. Une cochaîne harmonique $\varphi\in \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(n)}$ est appelée forme nouvelle (ou newform) si $\varphi\in \underline{H}_!^{\mathrm{new}}(\mathcal{T},\mathbb{Z})^{\Gamma_0(n)}$.

Nous allons maintenant rappeler l'application j qui sera utile dans la construction de la paramétrisation modulaire. Soient $v, w \in X(\mathcal{T})$ deux sommets. On note $g(v,w)$ l'unique géodésique allant de v à w. Pour $v \in X(\mathcal{T})$, $e \in Y(\mathcal{T})$ et $\gamma, \alpha \in \Gamma$, on pose

$$\iota(e,\alpha,\gamma,v) = \begin{cases} 1 & \text{si } \gamma e \in g(v,\alpha v), \\ -1 & \text{si } \gamma e \in g(\alpha v, v), \\ 0 & \text{sinon.} \end{cases}$$

Puisque l'application $\gamma \mapsto \iota(e,\alpha,\gamma,v)$ possède un support fini, la quantité

$$\varphi_{\alpha,v}(e) = \frac{1}{|\Gamma \cap \mathcal{Z}|} \sum_{\gamma \in \Gamma} \iota(e,\alpha,\gamma,v)$$

est bien définie et à valeurs dans $\mathbb{Z}$. On pose $\overline{\Gamma} = \Gamma^{\mathrm{ab}}/\operatorname{Tor}(\Gamma^{\mathrm{ab}})$, où Γ^{ab} est l'abélianisé de Γ et $\operatorname{Tor}(\Gamma^{\mathrm{ab}})$ est le sous-groupe de torsion de Γ^{ab}.

Lemme 68 ([26, lemme 3.3.3])**.** *Les fonctions $\varphi_{\alpha,v} : Y(\mathcal{T}) \to \mathbb{Z}$ possèdent les propriétés suivantes :*

1. *Pour tout $v \in X(\mathcal{T})$ et tout $\alpha \in \Gamma$, $\varphi_{\alpha,v} \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$.*
2. *La fonction $\varphi_\alpha = \varphi_{\alpha,v}$ est indépendante du choix de $v \in X(\mathcal{T})$.*
3. *L'application $\alpha \mapsto \varphi_\alpha$ induit un morphisme de groupes j de $\overline{\Gamma}$ dans $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$.*
4. *L'application $j\colon \overline{\Gamma} \to \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ est injective et de conoyau fini.*

Démonstration. Cette démonstration est faite dans [26]. Nous choisissons de la présenter car elle permet de déduire une méthode pour calculer l'image réciproque par j d'un élément de $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$. Cette méthode sera utilisée dans les sections 2.7 et 2.8.
La propriété (1) est évidente. Pour (2), il suffit de montrer que $\varphi_{\alpha,v} = \varphi_{\alpha,w}$ si v et w sont deux sommets voisins. Soient $v, w \in X(\mathcal{T})$ deux sommets voisins et $\alpha \in \Gamma$. Quitte à échanger v et w le graphe engendré par les géodésiques $g(v,\alpha v)$ et $g(w,\alpha w)$ est de l'une de ces deux formes :

$$\overset{v}{\bullet} \xrightarrow{e} \overset{w}{\bullet} \longrightarrow \cdots \overset{\alpha v}{\bullet} \xrightarrow{\alpha e} \overset{\alpha w}{\bullet}$$

$$\overset{v}{\bullet} \xrightarrow{e} \overset{w}{\bullet} \longrightarrow \cdots \overset{\alpha w}{\bullet} \xleftarrow{\alpha e} \overset{\alpha v}{\bullet}$$

On a donc $g(v,\alpha v) \cup \{\alpha(e)\} = \{e\} \cup g(w,\alpha w)$ ou $g(v,\alpha v) = \{e\} \cup g(w,\alpha w) \cup \{\overline{\alpha e}\}$. Dans le premier cas, pour une arête $e' \in Y(\mathcal{T})$ le même nombre de matrices dans Γ envoie e' sur e que e' sur αe. Pour le second cas, les contributions de e et de αe se compensent. Ainsi $\varphi_{\alpha,v} = \varphi_{\alpha,w}$. Pour (3), on a

$\varphi_{\alpha\beta,v} = \varphi_{\alpha,\beta v} + \varphi_{\beta,v}$ pour tout $\alpha, \beta \in \Gamma$ et tout $v \in X(\mathcal{T})$, donc (ii) implique que $\varphi_{\alpha\beta} = \varphi_\alpha + \varphi_\beta$. L'application $\Gamma \to \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ est donc un morphisme de groupes. Puisque $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ est un groupe abélien libre la dernière application se factorise en un morphisme $j\colon \overline{\Gamma} \to \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$.
Pour (4), remarquons tout d'abord que les groupes abéliens libres $\overline{\Gamma}$ et $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ sont tous deux de rang g, où g est le genre de $\overline{M}_\Gamma$. Il suffit donc de montrer que l'application $j \otimes \mathbb{Q}\colon \overline{\Gamma} \otimes \mathbb{Q} \to \underline{H}_!(\mathcal{T}, \mathbb{Q})^\Gamma$ est surjective. Soit $\mathfrak{T}$ un sous-arbre maximal de $\Gamma\backslash\mathcal{T}$, c'est à dire un sous-arbre tel que pour tout sous-arbre $\mathfrak{T}' \neq \mathfrak{T}$ de $\Gamma\backslash\mathcal{T}$, on a $\mathfrak{T} \not\subset \mathfrak{T}'$. Soient $\{\tilde{e}_1, ..., \tilde{e}_g\}$ un système de représentants de $Y(\Gamma\backslash\mathcal{T}) - Y(\mathfrak{T})$. Pour $i \in [\![1, g]\!]$, on note $\tilde{v}_i = o(\tilde{e}_i)$ et $\tilde{w}_i = t(\tilde{e}_i)$. Il existe une unique géodésique $\tilde{c}_i$ reliant $\tilde{w}_i$ à $\tilde{v}_i$. Soit $\tilde{g}_i$ le chemin de $\tilde{v}_i$ à $\tilde{v}_i$ obtenu en adjoignant $\tilde{e}_i$ à $\tilde{c}_i$. On définit ensuite

$$\varphi_i(\tilde{e}) = \begin{cases} n(e) & \text{si } \tilde{e} \in \tilde{g}_i \\ -n(e) & \text{si } \overline{\tilde{e}} \in \tilde{g}_i \\ 0 & \text{sinon,} \end{cases}$$

où $e \in Y(\mathcal{T})$ est un relèvement de $\tilde{e}$. On remarque que pour tout $i \in [\![1, g]\!]$, $\varphi_i \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$. Puisque $\varphi_i(\tilde{e}_j) = \delta_{i,j} n(e_j)$, les applications $(\varphi_i)_{1 \leq i \leq g}$ sont donc linéairement indépendantes. Soit $\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Q})^\Gamma$, l'application

$$\varphi - \sum_{i=1}^{g} \frac{\varphi_i(\tilde{e}_i)}{n(e_i)} \varphi_i$$

s'annule en dehors du sous-arbre $\mathfrak{T}$, et est donc identiquement nulle. Les applications $(\varphi_i)_{1 \leq i \leq g}$ forment donc une base de $\underline{H}_!(\mathcal{T}, \mathbb{Q})^\Gamma$. Soit maintenant g_i un relèvement dans $\mathcal{T}$ de $\tilde{g}_i$ d'origine $v_i \in \tilde{v}_i$ et de fin $v_i' \in \tilde{v}_i$. Il existe $\alpha_i \in \Gamma$ tel que $\alpha_i v_i = v_i'$ et on a $j(\alpha_i) = \varphi_i$, et donc $j \otimes \mathbb{Q}$ est surjective. □

De plus comme prouvé par Gekeler-Nonnengardt dans [25, Theorem 3.3], on a dans le cas du sous-groupe $\Gamma_0(n)$:

Théorème 69. *Soit $n \in A$ un polynôme non constant. Si $\Gamma = \Gamma_0(n)$ alors l'application $j\colon \overline{\Gamma} \to \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ est un isomorphisme.*

2.2.2 Développement en série de Fourier des formes automorphes

On s'intéresse maintenant au développement en série de Fourier des cochaînes harmoniques. On introduit d'abord le sous-groupe de Γ

$$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ a, d \in \mathbb{F}_q^*,\ b \in A \right\}.$$

On se place dans un cadre plus général en étudiant le développement d'une fonction

$$F\colon Y^+(\Gamma_\infty\backslash\mathcal{T}) \to \mathbb{C}.$$

À noter qu'une cochaîne harmonique $F \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ rentre dans ce cadre puisque $\Gamma_\infty \subset \Gamma_0(n)$ et qu'une telle application est entièrement déterminée par sa restriction aux arêtes positives. Pour un entier $k \in \mathbb{Z}$, le k-ième coefficient *constant* de F est défini par

$$c_0(\pi^k) = \begin{cases} F\left(\begin{pmatrix}\pi^k & 0\\ 0 & 1\end{pmatrix}\right) & \text{si } k \leq 1,\\ q^{1-k}\displaystyle\sum_{y\in\pi O_\infty/\pi^k O_\infty} F\left(\begin{pmatrix}\pi^k & y\\ 0 & 1\end{pmatrix}\right) & \text{si } k > 1.\end{cases}$$

Soit $\mathfrak{m}$ un diviseur positif de K. On écrit

$$\mathfrak{m} = \mathrm{div}(\mathfrak{m})\infty^{\deg(\mathfrak{m})}$$

où $\mathrm{div}(\mathfrak{m})$ est le diviseur principal de $m \in A$. Soit également $\eta\colon K_\infty \to \mathbb{C}$ l'application définie par

$$\eta\left(\sum_{i\in\mathbb{Z}} a_i\pi^i\right) = \eta_0 \circ \mathrm{Tr}(a_1),$$

où $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ est la trace et η_0 un caractère non trivial de $\mathbb{F}_p$.

Définition-Proposition 70. *Le $\mathfrak{m}$-ième coefficient de F est défini par*

$$c(\mathfrak{m}) = q^{-1-\deg(\mathfrak{m})} \sum_{y\in\pi O_\infty/\pi^{2+\deg(m)}O_\infty} F\left(\begin{pmatrix}\pi^{2+\deg(\mathfrak{m})} & y\\ 0 & 1\end{pmatrix}\right)\eta(-my).$$

Le développement de Fourier de F est

$$F\left(\begin{pmatrix}\pi^k & y\\ 0 & 1\end{pmatrix}\right) = c_0(\pi^k) + \sum_{\substack{m\in A, m\neq 0\\ \deg(m)\leq k-2}} c(\mathrm{div}(m)\infty^{k-2})\eta(my),\ k\in\mathbb{Z}, y\in K_\infty/\pi^k O_\infty.$$

On considère le caractère $\nu\colon K_\infty \to \mathbb{Z}$ qui à $\sum_{i\in\mathbb{Z}} a_i\pi^i$ associe -1 si $a_1 \neq 0$ et $q-1$ sinon. Le $\mathfrak{m}$-ième coefficient de Fourier de F peut se réécrire

$$c(\mathfrak{m}) = q^{-1-\deg(m)}\left(F\left(\begin{pmatrix}\pi^{2+\deg(m)} & 0\\ 0 & 1\end{pmatrix}\right) + \sum_{\substack{y\in\mathbb{F}_q^*\backslash\pi O_\infty/\pi^{2+\deg(m)}O_\infty\\ y\neq 0}} F\left(\begin{pmatrix}\pi^{2+\deg(m)} & y\\ 0 & 1\end{pmatrix}\right)\nu(my)\right),$$

et l'on peut réécrire F :

$$F\left(\begin{pmatrix}\pi^k & y\\ 0 & 1\end{pmatrix}\right) = c_0(\pi^k) + \sum_{\substack{m\in A, m \text{ unitaire}\\ \deg(m)\leq k-2}} c(\mathrm{div}(m\infty^{k-2}))\nu(my).$$

Lemme 71. *[21, 2.14] Soit F une fonction sur les arêtes de $\mathcal{T}$ à valeurs dans $\mathbb{C}$, alternée et Γ_∞-invariante. Alors F est harmonique si et seulement si ses coefficients de Fourier vérifient les conditions suivantes :*

1. *pour tout $k\in\mathbb{Z}$, $c_0(\pi^k) = q^{-k}c_0(1)$;*
2. *pour tout diviseur de la forme $\mathfrak{m} = \mathrm{div}(m)\infty^k$, $c(\mathfrak{m}) = c(\mathrm{div}(m))q^{-k}$.*

Corollaire 72. *[21, 2.14 et 3.1] Soit $F\in \underline{H}(\mathcal{T},\mathbb{C})^{\Gamma_\infty}$. Les coefficients c_0 de F sont tous nuls.*

Pour $\varphi\in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$, on notera désormais $c(\varphi,\cdot)$ ses coefficients de Fourier (à l'exception des coefficients c_0 puisque ceux-ci sont tous nuls).

2.3 Fonctions thêta pour Γ

Définition 73 ([26, Section 5])**.** *Une fonction* thêta holomorphe *(resp. fonction* thêta méromorphe*) pour Γ est une fonction holomorphe sur Ω sans zéros ni pôles sur Ω et aux pointes (resp. sans zéros ni pôles aux pointes), et satisfaisant*

$$f(\gamma z) = c_f(\gamma)f(z), \qquad \text{pour tout } z\in\Omega \text{ et } \gamma\in\Gamma,$$

avec $c_f(\gamma)\in\mathbb{C}_\infty^*$ indépendant de z. L'application $c_f\colon\Gamma\to\mathbb{C}_\infty^*$ est appelée le coefficient multiplicateur *de f.*

Soit m un entier positif. On pose $U_m = \{z\in\Omega, |z|\leq q^m,\ |z|_i\geq q^{-m}\}$. L'ensemble Ω est un sous-espace analytique rigide de $\mathbb{P}^1(\mathbb{C}_\infty)$ et $\Omega = \bigcup_{m\geq 1} U_m$ est un recouvrement admissible. Pour le reste de cette section, on fixe deux éléments $\omega,\eta\in\Omega$.

Définition 74. *On pose $\widetilde{\Gamma} = \Gamma/(\Gamma\cap\mathcal{Z})$ et*

$$\theta(\omega,\eta,z) = \prod_{\gamma\in\widetilde{\Gamma}} \frac{z-\gamma\omega}{z-\gamma\eta}. \tag{2.10}$$

Puisque $Z(\Gamma)\subset\mathcal{Z}$, le produit 2.10 est indépendant du système de représentants choisi pour $\widetilde{\Gamma}$.

Proposition 75. *[26, proposition 5.2.3] Le produit $\theta(\omega, \eta, z)$ converge uniformément localement sur Ω.*

Pour montrer cette proposition nous aurons besoin de plusieurs lemmes. Deux matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ de Γ définissent la même classe dans $\Gamma_\infty \backslash \Gamma$ si et seulement s'il existe $u \in \mathbb{F}_q^*$ tel que $(c', d') = u(c, d)$. On notera (c, d) la classe de γ dans $\Gamma_\infty \backslash \Gamma$.

Lemme 76. *[26, lemme 5.3.3] Soient c_0, c_1 deux constantes strictement positives. Pour presque toute classe (c, d) dans $\Gamma_\infty \backslash \Gamma$ d'éléments $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a : $|z|_i > c_0$ implique $|cz + d| > c_1$.*

Démonstration. Soient c_0, c_1 deux réels strictement positifs et soit $z \in \Omega$ tel que $|z|_i > c_0$. Pour tout $(c, d) \in \Gamma_\infty \backslash \Gamma$, on a $|cz + d| > |c||z|_i > c_1$, si $|c|$ est suffisamment grande. Pour le nombre fini de polynômes $c \in A$ ne vérifiant pas $|c||z|_i > c_1$, si $|d| > c_1$, on a $|cz + d| = |d| > c_1$. □

Lemme 77. *[26, corollaire 5.3.4] Soit $\varepsilon > 0$. Pour presque toute classe (c, d) tel que $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, on a $|\gamma\eta|_i < \varepsilon$.*

Démonstration. On a $|\gamma\eta|_i = \dfrac{|\eta|_i}{|c\eta + d|^2}$. On obtient le résultat en utilisant le lemme 76. □

Lemme 78. *Soit $(c, d) \in \Gamma_\infty \backslash \Gamma$ fixé et c_2, c_3 deux constantes strictement positives. Pour presque toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $|z| < c_2$ implique $|z - \gamma\eta| > c_3$.*

Démonstration. On applique le lemme 76 à $z = \eta$ et (a, b), pour presque tout couple (a, b), on a

$$|\gamma\eta| = |c\eta + d|^{-1}|a\eta + b| > \max(c_2, c_3).$$

Ainsi $|z - \gamma\eta| = |\gamma\eta| > c_3$. □

Lemme 79. *[26, lemme 5.3.6] Soit $\eta \in \Omega$ fixé. Pour presque tout $\gamma \in \Gamma$, on a $|z - \gamma\eta| \geq q^{-n}$, pour tout $z \in U_n$.*

Démonstration. Par le lemme 77, on a $|\gamma\eta|_i < q^{-n}$ pour presque toute classe $(c, d) \in \Gamma_\infty \backslash \Gamma$, pour $\gamma \in (c, d)$ on a

$$|z - \gamma\eta| \geq |z - \gamma\eta|_i \geq q^{-n}$$

Pour les classes (c, d) restantes on applique le lemme 78. □

Lemme 80. *[26, lemme 5.3.8] Soient $n \in \mathbb{N}^*$ et $\varepsilon > 0$. Pour presque tout $\gamma \in \Gamma$, pour tout $z \in U_n$, on a*

$$\left|\frac{z-\gamma\omega}{z-\gamma\eta} - 1\right| < \varepsilon.$$

Démonstration. On a

$$\left|\frac{z-\gamma\omega}{z-\gamma\eta} - 1\right| = \frac{|\eta-\omega|}{|z-\gamma\eta||c\eta+d||c\omega+d|}. \tag{2.11}$$

Soit $\kappa > 0$. Par les lemmes 79 et 77 pour presque toute classe (c,d), on a

$$\frac{1}{|c\eta+d||c\omega+d|} < \frac{\kappa q^n}{|\eta-\omega|}.$$

Pour les classes (c,d) restantes on applique le lemme 78. □

Proposition 81. *[26, lemme 5.3.9] Soit $s = \frac{u}{v} \in K$. Le produit*

$$\prod_{\gamma\in\tilde{\Gamma}} \frac{s-\gamma\omega}{s-\gamma\eta},$$

converge.

Démonstration. Pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, on a

$$|s-\gamma\eta| = \frac{|(uc-av)\eta + ud - bv|}{|v||c\eta+d|} \geq c_4|c\eta+d|^{-1},$$

avec c_4 une constante indépendante de $\gamma \in \Gamma$. Il vient que

$$\left|\frac{s-\gamma\omega}{s-\gamma\eta} - 1\right| \leq c_4^{-1}\frac{|\eta-\omega|}{|c\omega+d|}.$$

Comme précédemment pour presque toute classe (c,d) la dernière quantité est inférieure à ε. Pour les classes (c,d) restantes on applique le lemme 78. □

Lemme 82. *[26, lemme 5.3.10] Soient $\omega, \eta \in \Omega$ et soit $\varepsilon > 0$. Il existe $c_5 > 0$ telle que pour tout $\gamma \in \tilde{\Gamma}$ et tout $|z|_i > c_5$:*

$$\left|\frac{z-\gamma\omega}{z-\gamma\eta} - 1\right| \leq \varepsilon.$$

Démonstration. On a

$$\left|\frac{z-\gamma\omega}{z-\gamma\eta}-1\right| \leq \frac{c_6}{|z-\gamma\eta|},$$

où c_6 dépend uniquement de ω et η. Posons donc $c_5 = \sup\{\frac{c_6}{\varepsilon}, |\gamma\eta|_i, \gamma \in \tilde{\Gamma}\}$. On a alors pour $|z|_i > c_5$:

$$|z-\gamma\eta| \geq |z-\gamma\eta|_i \geq |z|_i \geq c_5,$$

donc $\left|\frac{z-\gamma\omega}{z-\gamma\eta}-1\right| \leq \varepsilon$. □

Remarque. Dans [23], on voit qu'on peut également définir les fonctions $\theta(\omega,\eta,.)$ avec $\omega,\eta \in \overline{\Omega} = \Omega \cup \mathbb{P}^1(K)$. On définit la fonction rationnelle $G(\omega,\eta,z)$ par

$$G(\omega,\eta,z) = \begin{cases} \dfrac{z-\omega}{z-\eta} & \text{si } \omega \neq \infty \neq \eta \\ \left(1-\frac{z}{\eta}\right)^{-1} & \text{si } \omega = \infty, \eta \notin \{0,\infty\} \\ 1-\frac{z}{\omega} & \text{si } \eta = \infty, \omega \notin \{0,\infty\} \\ z^{-1} & \text{si } \omega = \infty, \eta = 0 \\ z & \text{si } \eta = \infty, \omega = 0 \\ 1 & \text{si } \omega = \eta = \infty. \end{cases}$$

On pose alors

$$\theta(\omega,\eta,z) = \prod_{\gamma\in\tilde{\Gamma}} G(\gamma\omega,\gamma\eta,z).$$

La fonction ainsi définie converge uniformément localement sur Ω. À noter que les fonctions $\theta(\omega,\eta,.)$ sont des fonctions méromorphes sur Ω comme limites uniformes de fonctions rationnelles sur Ω. D'autre part par la proposition 9, le produit $\prod_{\gamma\in\tilde{\Gamma}} \frac{z-\gamma\omega}{z-\gamma\eta}$ est indépendant de l'ordre choisi.

Proposition 83. *[26, théorème 5.4.1] Soient $\omega,\eta \in \Omega$ et $\alpha \in \Gamma$. Alors*

1. *Il existe une constante $c(\omega,\eta,\alpha) \in \mathbb{C}_\infty^*$ appelé coefficient multiplicateur tel que*
$$\theta(\omega,\eta,\alpha z) = c(\omega,\eta,\alpha)\theta(\omega,\eta,z),$$
où $c(\omega,\eta,\alpha)$ est indépendant de $z \in \Omega$.
2. *Le coefficient $c(\omega,\eta,\alpha)$ dépend uniquement de la classe de $\alpha \in \overline{\Gamma}$. Donc l'application $\alpha \mapsto c(\omega,\eta,\alpha)$ définit un morphisme de groupes de Γ dans $\mathbb{C}_\infty$ qui se factorise sur $\overline{\Gamma}$.*

3. *La fonction u_α définie par*

$$u_\alpha(z) = \theta(\omega, \alpha\omega, z) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{z - \gamma\omega}{z - \gamma\alpha\omega} \tag{2.12}$$

est indépendante du choix de $\omega \in \Omega$.

4. *Soit $\beta \in \Gamma$. On a $u_{\alpha\beta} = u_\alpha u_\beta$.*

5. *On a l'équation fonctionnelle suivante :*

$$c(\omega, \eta, \alpha) = \frac{u_\alpha(\eta)}{u_\alpha(\omega)}. \tag{2.13}$$

6. *Soit $c_\alpha(.)$ le coefficient multiplicateur de u_α. L'application*

$$\begin{array}{ccc} \overline{\Gamma} \times \overline{\Gamma} & \to & \mathbb{C}_\infty^* \\ (\alpha, \beta) & \mapsto & c_\alpha(\beta) \end{array}$$

est bilinéaire symétrique et à valeurs dans K_∞^*.

Démonstration. 1. Soit $\alpha \in \Gamma$, on a

$$\frac{\alpha z - \gamma\omega}{\alpha z - \gamma\eta} = h_\alpha(\gamma) \frac{z - \alpha^{-1}\gamma\omega}{z - \alpha^{-1}\gamma\eta}$$

où

$$h_\alpha(\gamma) = \begin{cases} 1 & \text{si } \alpha\infty = \infty \\ \dfrac{\alpha\infty - \gamma\omega}{\alpha\infty - \gamma\eta} & \text{si } \alpha\infty \neq \infty. \end{cases}$$

Ainsi $u_\alpha(z) = \prod_{\gamma \in \Gamma} h_\alpha(\gamma) \dfrac{z - \alpha^{-1}\gamma\omega}{z - \alpha^{-1}\gamma\eta}$. Il suffit donc de montrer que le produit $c(\omega, \eta, \alpha) = \prod_{\gamma \in \Gamma} h_\alpha(\gamma)$ converge. Pour α telle que $\alpha\infty = \infty$, le résultat est trivial et pour $\alpha\infty = \frac{u}{v} \in K$, c'est la proposition 81.

2. Puisque l'application $\alpha \mapsto c(\omega, \eta, \alpha)$ est un morphisme de groupes à valeurs dans le groupe abélien $\mathbb{C}_\infty^*$, elle se factorise sur Γ^{ab}.
Soit $\beta \in \Gamma^{\mathrm{ab}}$ d'ordre $m \in \mathbb{N}^*$. La fonction holomorphe $\eta \mapsto c(\omega, \eta, \beta)$ est à valeurs dans les racines m-ièmes de l'unité, donc est constante. Puis en substituant η par ω on obtient que l'application est constante égale 1.

3. Soient $\omega, \eta \in \Omega$. On a

$$\begin{aligned}\theta(\omega, \alpha\omega, z)\theta(\eta, \alpha\eta, z)^{-1} &= \prod_{\gamma\in\tilde{\Gamma}} \frac{z-\gamma\omega}{z-\gamma\alpha\omega} \prod_{\gamma\in\tilde{\Gamma}} \frac{z-\gamma\alpha\eta}{z-\gamma\eta} \\ &= \prod_{\gamma\in\tilde{\Gamma}} \frac{z-\gamma\omega}{z-\gamma\eta} \prod_{\gamma\in\tilde{\Gamma}} \frac{z-\gamma\alpha\eta}{z-\gamma\alpha\omega} \\ &= \theta(\omega, \eta, z)\theta(\eta, \omega, z) = 1.\end{aligned}$$

4. Pour tout $z \in \Omega$,

$$u_{\alpha\beta}(z) = \theta(\omega, \alpha\beta\omega, z) = \theta(\omega, \beta\omega, z)\theta(\beta\omega, \alpha\beta\omega, z) = u_\alpha(z)u_\beta(z).$$

5. Soit $\Omega - (\Gamma\omega \cup \Gamma\eta)$. On a

$$c(\omega, \eta, \alpha) = \frac{\theta(\omega, \eta, \alpha z)}{\theta(\omega, \eta, z)} = \prod_{\gamma\in\tilde{\Gamma}} \frac{\frac{\alpha z-\gamma\omega}{\alpha z-\gamma\eta}}{\frac{z-\gamma\omega}{z-\gamma\eta}}.$$

Le γ-ième facteur du produit précédent vérifie

$$\frac{\frac{\alpha z-\gamma\omega}{\alpha z-\gamma\eta}}{\frac{z-\gamma\omega}{z-\gamma\eta}} = \frac{\frac{\gamma\omega-\alpha z}{\gamma\omega-z}}{\frac{\gamma\eta-\alpha z}{\gamma\eta-z}} = \frac{\frac{\omega-\gamma^{-1}\alpha z}{\omega-\gamma^{-1}z}}{\frac{\eta-\gamma^{-1}\alpha z}{\eta-\gamma^{-1}z}} = \frac{\eta-\gamma^{-1}z}{\eta-\gamma^{-1}\alpha z}\left(\frac{\omega-\gamma^{-1}z}{\omega-\gamma^{-1}\alpha z}\right)^{-1}$$

Finalement

$$\prod_{\gamma\in\tilde{\Gamma}} \frac{\eta-\gamma^{-1}z}{\eta-\gamma^{-1}\alpha z}\left(\frac{\omega-\gamma^{-1}z}{\omega-\gamma^{-1}\alpha z}\right)^{-1} = \frac{u_\alpha(\eta)}{u_\alpha(\omega)}.$$

6. Puisque pour tout $\alpha \in \Gamma$, l'application $\gamma \in \Gamma \mapsto c_\alpha(\gamma) \in \mathbb{C}_\infty^*$ se factorise sur $\overline{\Gamma}$, l'application

$$\begin{array}{rccc} c\colon & \Gamma & \longrightarrow & \mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*) \\ & \alpha & \longmapsto & c_\alpha(.) \end{array}$$

est bien définie. D'autre part, l'application c se factorise $\overline{\Gamma}$ et donne une application $\bar{c}\colon \overline{\Gamma} \to \mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*)$. Soit $\omega \in \Omega$ un élément algébrique sur K_∞. On a que $c_\alpha(\beta) \in K_\infty(\omega)$. Puisque le produit définissant u_α est indépendant du choix $\omega \in \Omega$, il vient que

$$c_\alpha(\beta) \in \bigcap_{\substack{\omega\in\Omega \\ \omega \text{ algbrique sur } K_\infty}} K_\infty(\omega),$$

et donc que $c_\alpha(\beta) \in K_\infty$.

□

Théorème 84 ([23, Proposition 2.6]). *Soit ω, η des éléments de Ω. La fonction $\theta(\omega, \eta, .)$ possède un prolongement méromorphe aux pointes $\mathbb{P}^1(K)$ de Ω. De plus, $\theta(\omega, \eta, .)$ est holomorphe non nulle aux pointes.*

Remarque. La valeur du prolongement méromorphe de $\theta(\omega, \eta, .)$ en la pointe ∞ est 1 (cela provient de [26, lemme 5.3.10]).

2.4 Évaluation des fonctions thêta aux pointes

Une conséquence du théorème 84 est que la fonction holomorphe u_α possède un prolongement holomorphe sur $\overline{\Omega} = \Omega \sqcup \mathbb{P}^1(K)$ donc est une fonction thêta holomorphe. D'autre part, comme établi dans [26, lemme 5.3.9] et dans la proposition 81, pour tout $s \in K$ et tout $\omega, \eta \in \Omega$, le produit $\displaystyle\prod_{\gamma \in \widetilde{\Gamma}} \frac{s - \gamma\omega}{s - \gamma\eta}$ converge. On remarque que cela n'implique pas nécessairement que l'image de u_α en une pointe $s \in K$ est donnée par la formule (2.12). Cependant nous prouvons maintenant que c'est bien le cas.

Théorème 85. *Soit α un élément de $\overline{\Gamma}$ et $s \in \mathbb{P}^1(K) - \{\infty\}$. La valeur de u_α en s est donnée par*

$$u_\alpha(s) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{s - \gamma\omega}{s - \gamma\alpha\omega}.$$

Le reste de cette section est consacrée à la preuve du théorème 85. Soit $s \in \mathbb{P}^1(K) - \{\infty\}$. Puisque le produit $u_\alpha(z)$ est indépendant du choix de $\omega \in \Omega$, on peut choisir $\omega \in \Omega$ tel que $|\omega| \in q^{\mathbb{Q}-\mathbb{Z}}$. Cela implique que $|\omega| = |\omega|_i$. Pour $z \in \overline{\Omega}$, $\gamma \in \Gamma$, on note $G_{\gamma,\omega}(z)$:

$$G_{\gamma,\omega}(z) = \frac{z - \gamma\omega}{z - \gamma\alpha\omega}.$$

On a

$$\left| \prod_{\gamma \in \widetilde{\Gamma}} G_{\gamma,\omega}(s) - \prod_{\gamma \in \widetilde{\Gamma}} G_{\gamma,\omega}(z) \right| = |u_\alpha(z)| \left| \prod_{\gamma \in \widetilde{\Gamma}} \frac{(s - \gamma\omega)(z - \gamma\alpha\omega)}{(s - \gamma\alpha\omega)(z - \gamma\omega)} - 1 \right|. \quad (2.14)$$

On pose $F_{\gamma,s}(z) = \dfrac{(s - \gamma\omega)(z - \gamma\alpha\omega)}{(s - \gamma\alpha\omega)(z - \gamma\omega)}$.

Lemme 86. *Pour* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}$, *on a*

$$F_{\gamma,s}(z) = 1 + \frac{(z-s)(\alpha\omega - \omega)\det(\gamma)}{(s-\gamma\alpha\omega)(z-\gamma\omega)(c\omega+d)(c\alpha\omega+d)}.$$

Démonstration. Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}$ et $z \in \Omega$. On commence par remarquer que

$$\gamma\alpha\omega - \gamma\omega = \frac{(\alpha\omega - \omega)\det(\gamma)}{(c\omega+d)(c\alpha\omega+d)}. \tag{2.15}$$

D'autre part, on a

$$\begin{aligned} \frac{(s-\gamma\omega)(z-\gamma\alpha\omega)}{(s-\gamma\alpha\omega)(z-\gamma\omega)} &= \frac{sz - s(\gamma\alpha\omega) - z(\gamma\omega) + (\gamma\omega)(\gamma\alpha\omega)}{(s-\gamma\alpha\omega)(z-\gamma\omega)} \\ &= 1 + \frac{(z-s)(\gamma\alpha\omega - \gamma\omega)}{(s-\gamma\alpha\omega)(z-\gamma\omega)} \\ &= 1 + \frac{(z-s)(\alpha\omega-\omega)\det(\gamma)}{(s-\gamma\alpha\omega)(z-\gamma\omega)(c\omega+d)(c\alpha\omega+d)} \end{aligned}$$

et le lemme suit. □

On sait que $|s - \gamma\alpha\omega| \geq \frac{\kappa_{s,\alpha\omega}}{|c\alpha\omega+d|}$ (voir preuve de la proposition 81) où $\kappa_{s,\alpha\omega}$ est un réel positif qui dépend seulement de s, α et ω. Il vient que

$$|F_{\gamma,s}(z) - 1| \leq \frac{|z-s||\alpha\omega-\omega|\kappa_{s,\alpha\omega}^{-1}}{|z-\gamma\omega||c\omega+d|} \leq \frac{|z-s|C_{\omega,\alpha,s}}{|z-\gamma\omega||c\omega+d|} \tag{2.16}$$

où $C_{\omega,\alpha,s}$ est indépendant de $\gamma \in \Gamma$ et de $z \in \Omega$.

Le but est de prouver que (2.14) tend vers 0 lorsque z tend vers s. Du prolongement méromorphe de u_α en s, on déduit que $u_\alpha(z) \underset{z\to s}{\to} u_\alpha(s)$. Il suffit donc de trouver une suite $(z_n)_{n\in\mathbb{N}} \subset \Omega$ telle que $\lim_{n\to\infty} z_n = s$ et telle que

$$\lim_{n\to\infty} u_\alpha(z_n) = \prod_{\gamma\in\widetilde{\Gamma}} \frac{s-\gamma\omega}{s-\gamma\alpha\omega}. \tag{2.17}$$

On a

$$|u_\alpha(z_n)| \leq \max(|u_\alpha(s)|, |u_\alpha(s) - u_\alpha(z_n)|) < C \tag{2.18}$$

où $C > 0$ dépend uniquement de s et α puisque $u_\alpha(z_n) \to u_\alpha(s)$. Maintenant pour montrer (2.17), nous devons montrer que pour tout $\varepsilon > 0$, il existe $n_\varepsilon > 0$ tel que pour tout $n \geq n_\varepsilon$, $|F_{\gamma,s}(z_n) - 1| < \varepsilon$. On choisit $\zeta \in \Omega - \Gamma\omega$ tel que $|\zeta| = |\zeta|_i = 1$ et on pose $z_n = s + T^{-n}\zeta$. On remarque que $|z_n|_i = q^{-n}$ pour tout entier positif n.

Lemme 87. *Soit $\varepsilon > 0$ un nombre réel. Il existe un entier positif n_0 tel que pour tout $n \geq n_0$, si γ satisfait $|z_n - s|_i > |\gamma\omega|_i$ alors $|F_{\gamma,s}(z_n) - 1| \leq \varepsilon$.*

Démonstration. Soit $\varepsilon > 0$ fixé et $n \geq 0$. On commence par remarquer que $|c\omega + d| \geq |c\omega|_i = |c||\omega|_i$.
Donc, si $|c| > |\omega|_i^{-1} q^n$ ou si $|d| > \max\left(|c\omega|, \left(|\omega|_i^{-1} q^n\right)^{\frac{1}{2}}, q^n\right)$, on a

$$|\gamma\omega|_i = \frac{|\omega|_i}{|c\omega + d|^2} < |z_n - s|_i = q^{-n}.$$

Pour les paires (c, d) satisfaisant au moins l'une des deux conditions sur $|c|$ ou $|d|$, on a $|c\omega + d| > q^n$ et puisque $|\gamma\omega|_i < |z_n - s|_i$ on a

$$|z_n - \gamma\omega| \geq |z_n - s - \gamma\omega|_i = |z_n - s|_i.$$

Donc on obtient

$$\begin{aligned} |F_{\gamma,s}(z_n) - 1| &\leq \frac{|z_n - s| C_{\omega,\alpha,s}}{|z_n - s|_i |c\omega + d|} \qquad \text{par (2.16)} \\ &\leq \frac{C_{\omega,\alpha,s}}{|c\omega + d|} \leq C_{\omega,\alpha,s} q^{-n} \end{aligned}$$

qui est inférieur ou égal à ε lorsque n est assez grand. □

Lemme 88. *Soit $\varepsilon > 0$ un nombre réel. Il existe $n_1 \geq 0$ tel que pour tout entier $n \geq n_1$, si $\gamma \in \Gamma$ vérifie $|\gamma\omega|_i > |z_n - s|_i$ alors $|F_{\gamma,s}(z_n) - 1| \leq \varepsilon$.*

Démonstration. Soit $\varepsilon > 0$ fixé et $n \geq 0$ un entier suffisamment grand. Si $\gamma \in \Gamma$ vérifie $|\gamma\omega|_i > |z_n - s|_i$ alors $|s - \gamma\omega| \geq |\gamma\omega|_i > |z_n - s|_i = |z_n|_i = |z_n - s|$. Par l'inégalité ultramétrique, on a

$$|z_n - \gamma\omega| = |(z_n - s) + s - \gamma\omega| = |s - \gamma\omega| \geq \frac{\kappa_{\omega,s}}{|c\omega + d|},$$

où $\kappa_{\omega,s}$ est indépendant de $\gamma \in \Gamma$ (voir preuve de la proposition 81). Par (2.16), on obtient alors $|F_{\gamma,s}(z_n) - 1| \leq |z_n - s| C_{\omega,\alpha,s} \kappa_{\omega,s}^{-1}$, ce qui est inférieur ou égal à ε si n est suffisamment grand. □

Corollaire 89. *Soit $\varepsilon > 0$. Il existe $n_2 \geq 0$ tel que pour tout $n \geq n_2$ et tout $\gamma \in \Gamma$, on a $|F_{\gamma,s}(z_n) - 1| \leq \varepsilon$.*

Démonstration. Soit $\varepsilon > 0$ fixé. On pose $n_2 = \max(n_0, n_1)$ où n_0 et n_1 sont pris comme dans les lemmes 87 et 88. On obtient $|F_{\gamma,s}(z_n) - 1| < \varepsilon$ lorsque $|\gamma\omega|_i \neq |z_n - s|_i$. De plus, puisque $|\omega| = |\omega|_i \in q^{\mathbb{Q}-\mathbb{Z}}$, pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}$ on a $|c\omega + d| = \max(|c\omega|, |d|)$. Ainsi, on obtient $|\gamma\omega|_i \in q^{\mathbb{Q}-\mathbb{Z}}$ pour tout $\gamma \in \widetilde{\Gamma}$, et donc $|\gamma\omega|_i \neq |z_n - s|_i = q^{-n}$. □

Par le corollaire 89, il existe n_2 tel que pour tout $n \geq n_2$,

$$\left| \prod_{\gamma \in \widetilde{\Gamma}} \frac{s - \gamma\omega}{s - \gamma\alpha\omega} - \prod_{\gamma \in \widetilde{\Gamma}} \frac{z_n - \gamma\omega}{z_n - \gamma\alpha\omega} \right| \leq C\varepsilon,$$

où la constante C est la même que dans (2.18). Cela conclut la preuve du théorème 85.

2.5 Opérateurs de Hecke

À partir de maintenant, le sous-groupe Γ sera toujours de la forme $\Gamma_0(n)$ avec $n \in A$ non constant et unitaire. Soit $\varphi \in \underline{H}(\mathcal{T}, B)^\Gamma$ où $B = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. On considère φ comme une application sur $\mathrm{Gl}_2(K_\infty)$. Soit $\mathfrak{m} = (m) \subset A$ un idéal. On pose

$$T_\mathfrak{m}(\varphi)(e) = \sum_{\substack{a,b,d \in A \\ a \text{ unitaire} \\ \deg(d) < \deg(b) \\ ad = m, (a,n) = 1}} \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} e \right) \qquad (e \in E(\mathcal{T})).$$

On a alors $T_\mathfrak{m}(\varphi) \in \underline{H}(\mathcal{T}, B)^\Gamma$ et l'opérateur $T_\mathfrak{m}$ est appelé le $\mathfrak{m}$-ième opérateur de Hecke. Le résultat classique suivant peut être trouvé par exemple dans [22, Section 7].

Proposition 90. *Les opérateurs de Hecke satisfont les propriétés suivantes :*

1. *Soit $\mathfrak{p} \subset A$ un idéal premier et k un entier positif. Alors $T_{\mathfrak{p}^k}$ est un polynôme en $T_\mathfrak{p}$.*
2. *Soit $\mathfrak{m}, \mathfrak{m}'$ deux idéaux de A premiers entre eux, alors $T_{\mathfrak{m}\mathfrak{m}'} = T_\mathfrak{m} T_{\mathfrak{m}'}$.*
3. *Les opérateurs de Hecke commutent deux à deux.*

Il est également possible de définir une action de Hecke sur $\overline{\Gamma}$ (voir [26, 9.3]). Si $\mathfrak{p} = (P)$ est un idéal de A premier à n, on pose

$$\tau_P = \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Gl}_2(K_\infty)$$

et on définit

$$\Delta_P = \Gamma \cap \tau_P \Gamma \tau_P^{-1}.$$

Pour $\alpha \in \overline{\Gamma}$, on définit $T_\mathfrak{p}(\alpha)$ comme

$$T_\mathfrak{p}(\alpha) = \tau_P^{-1} \prod_{\alpha_i \in \Delta_P \backslash \Gamma} \alpha_i \alpha \alpha_{\sigma(i)}^{-1} \tau_P \tag{2.19}$$

où α_i parcourt un système de représentants de $\Delta_P\backslash\Gamma$ et σ est la permutation de $\Delta_P\backslash\Gamma$ telle que $\alpha_i\alpha\alpha_{\sigma(i)}^{-1} \in \Delta_P$.

Lemme 91 ([26, Lemma 9.3.2]). *Soit $\mathfrak{a} = (a)$ un idéal A premier à n et $\alpha \in \Gamma$. On a $j(T_\mathfrak{a}(\alpha)) = T_\mathfrak{a}(j(\alpha))$. En d'autres termes, l'action des opérateurs de Hecke commute avec l'isomorphisme j.*

Proposition 92 ([26, Lemma 9.3.3]). *Les opérateurs de Hecke sur $\overline{\Gamma}$ définis dans* (2.19) *sont autoadjoints par rapport à l'application bilinéaire $(\alpha, \beta) \mapsto c_\alpha(\beta)$.*

Soit J_Γ la jacobienne de $\overline{M}_\Gamma$. C'est une variété abélienne sur K de dimension $g(\Gamma)$ où $g(\Gamma)$ est le genre de la courbe modulaire $\overline{M}_\Gamma$.

Définition 93 ([18, VIII,1]). *Soit $\mathfrak{p} = (P)$ un idéal premier de A et Δ_P, τ_P comme précédemment. Le $\mathfrak{p}$-ième opérateur de Hecke sur $\overline{M}_\Gamma$ est donné par la correspondance*

$$T_\mathfrak{p}\omega = \sum_{\alpha\in\Delta_P\backslash\Gamma} \tau_P^{-1}\alpha\omega, \qquad \omega \in \overline{M}_\Gamma(\mathbb{C}_\infty).$$

L'action des opérateurs de Hecke sur $\overline{M}_\Gamma$ induit une action sur J_Γ. En effet si $D = \sum a_i(\omega_i) \in J_\Gamma(\mathbb{C}_\infty)$ alors $T_\mathfrak{p}(D) = \sum a_i(T_\mathfrak{p}(\omega_i))$ (voir [18, Chapter VIII] pour plus de détails). L'action des opérateurs de Hecke $J_\Gamma(\mathbb{C}_\infty)$ induit l'action suivante sur $\mathbb{C}_\infty^*/t^{\mathbb{Z}} \simeq E(\mathbb{C}_\infty)$ (voir [26, 9.4 et 9.5.6])

$$T_\mathfrak{m}u_\alpha(z) = \prod_{\substack{a,b,d\in A\\ a \text{ unitaire}\\ \deg(d)<\deg(b)\\ ad=m,(a,n)=1}} u_\alpha\left(\frac{az+b}{d}\right). \tag{2.20}$$

2.6 Paramétrisation modulaire

Proposition 94 ([26, 7.3.3]). *La variété de groupe analytique* $\mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*)/c(\overline{\Gamma})$ *possède une structure d'une variété abélienne K_∞-isomorphe à J_Γ.*

En d'autres termes, on a la suite exacte

$$1 \to \overline{\Gamma} \xrightarrow{\bar{c}} \mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*) \to J_\Gamma(\mathbb{C}_\infty) \to 0. \tag{2.21}$$

Les opérateurs Hecke agissent sur chacun de ses termes et l'application $\bar{c}\colon \overline{\Gamma} \to \mathbb{C}_\infty$ est compatible avec leurs actions (voir [26, 9.3.3]). Il en va de même pour la projection $\mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*) \to J_\Gamma(\mathbb{C}_\infty)$.

Soit E/K une courbe elliptique de mauvaise réduction multiplicative en la place $\infty = 1/T$ de K. De manière équivalente, E possède une paramétrisation de Tate multiplicative

$$E(K_\infty) \simeq K_\infty^*/t^{\mathbb{Z}}, \tag{2.22}$$

pour un certain $t \in K_\infty^*$ vérifiant $|t| < 1$. Pour tout idéal premier $\mathfrak{p}$, on note $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$, et $\overline{E}$ la réduction de E modulo $\mathfrak{p}$. On pose $\lambda_\mathfrak{p} = q^{\deg(\mathfrak{p})}+1-\#\overline{E}(\mathbb{F}_\mathfrak{p})$ si E a bonne réduction en $\mathfrak{p}$, et si E est de mauvaise réduction en $\mathfrak{p}$, on pose :

$$\lambda_\mathfrak{p} = \begin{cases} 1 & \text{si } E \text{ est de mauvaise réduction multiplicative déployée en } \mathfrak{p} \\ -1 & \text{si } E \text{ est de mauvaise réduction multiplicative non déployée en } \mathfrak{p} \\ 0 & \text{sinon.} \end{cases}$$

Depuis les travaux Weil, Jacquet-Langlands, Deligne, Grothendieck, Drinfeld et Zarhin, on a le résultat suivant :

Théorème 95. *[26, 8.3] Soit E une courbe elliptique définie sur $\mathbb{F}_q(T)$ de mauvaise réduction multiplicative déployée en la place $\infty = 1/T$. Alors il existe une unique forme nouvelle $\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ non divisible telle que*

$$\begin{cases} c(\varphi, 1) = 1 \\ T_\mathfrak{m}(\varphi) = q^{\deg(\mathfrak{m})} c(\varphi, \mathfrak{m})\varphi & \text{pour tout idéal } \mathfrak{m} \subset A, \\ c(\varphi, \mathfrak{p}) = q^{-\deg(\mathfrak{p})}\lambda_\mathfrak{p} & \text{pour tout idéal premier } \mathfrak{p} \subset A. \end{cases}$$

On identifie $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ avec $\overline{\Gamma}$ au moyen de l'isomorphisme j du théorème 69. On peut considérer φ comme un élément de $\overline{\Gamma}$.

Proposition 96 ([26, Proposition 9.5.1], [20, Theorem 3.2])**.** *Soit ev_φ l'application d'évaluation en φ de $\mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*)$ dans $\mathbb{C}^*$. Le sous-groupe $\mathrm{ev}_\varphi(c(\overline{\Gamma}))$ est isomorphe à $\mathbb{Z}$ et engendré par un unique $t \in K_\infty^*$ vérifiant $|t| < 1$.*

Soit $\Lambda = \{c_\varphi(\gamma), \gamma \in \Gamma\} = t^{\mathbb{Z}}$. On a le diagramme commutatif suivant

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{\Gamma} & \xrightarrow{\bar{c}} & \mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty^*) & \longrightarrow & J_\Gamma(\mathbb{C}_\infty) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle c_\varphi(.)} & & \downarrow{\scriptstyle \mathrm{ev}_\varphi} & & \downarrow & & \\ 1 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_\infty^* & \longrightarrow & \mathbb{C}_\infty^*/\Lambda & \longrightarrow & 0 \end{array} \tag{2.23}$$

Définition 97. *[20, 3.4] La paramétrisation modulaire (aussi appelée uniformisation de Weil) est définie comme*

$$\begin{array}{rccc} \Phi\colon & \overline{M}_\Gamma(\mathbb{C}_\infty) & \longrightarrow & \mathbb{C}_\infty^*/\Lambda \simeq E_\varphi(\mathbb{C}_\infty) \\ & z & \longmapsto & u_\varphi(z), \end{array}$$

où E_φ est appelée la courbe de Weil associée à la cochaîne harmonique φ.

Remarque. La courbe E_φ est une courbe de Weil forte c'est à dire Φ ne peut être factorisée par une autre uniformisation de Weil

$$\Phi' \colon \overline{M}_\Gamma(\mathbb{C}_\infty) \stackrel{\Phi'}{\to} E'(\mathbb{C}_\infty) \to E_\varphi(\mathbb{C}_\infty),$$

où E' est une courbe elliptique.

On pose

$$\mu = \inf\{\langle\varphi,\psi\rangle > 0,\ \psi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma\} = \inf\{\log_q|c_\varphi(\gamma)| > 0,\ \gamma \in \overline{\Gamma}\}.$$

Gekeler a montré que $\mu = v_\infty(t) = -v_\infty(j_E)$ où j_E est le j-invariant de E_φ ([20, Théorème 3.2, Corollaire 3.19]). Rappelons aussi sa formule pour calculer le degré de la paramétrisation modulaire.

Théorème 98 ([20, Proposition 3.8])**.** *Le degré de la paramétrisation modulaire Φ est donnée par*

$$\deg(\Phi) = \frac{\langle\varphi,\varphi\rangle}{\mu}.$$

On veut calculer les valeurs prises par la paramétrisation modulaire Φ en les pointes de $\overline{M}_\Gamma$. Par un analogue du théorème de Manin-Drinfeld, prouvé dans ce cadre par Gekeler [24, Théorème 1.2], le sous-groupe de la jacobienne de $\overline{M}_\Gamma$ engendré par les les pointes est fini. Par conséquent, l'image des pointes par Φ sont des points de torsion de la courbe elliptique. Cependant, le résultat de Gekeler ne fournit aucune borne explicite pour la taille du sous-groupe cuspidal en général. Pour notre propos, nous prouvons une borne explicite sur l'ordre de ces points de torsion : la borne dépend de la courbe elliptique et est prouvée en utilisant les opérateurs de Hecke et le même principe de preuve que Manin-Drinfeld.

Théorème 99. *Soit $s \in \Gamma\backslash\mathbb{P}^1(K)$ une pointe de M_Γ. Alors $\Phi(s)$ est un point de torsion $E(K_\infty)$ et son ordre divise $\#(\overline{E}(\mathbb{F}_\mathfrak{p}))$ pour tout $\mathfrak{p} = (P)$ vérifiant $P \equiv 1 \bmod n$.*

Démonstration. Soit $z \in \overline{M}_\Gamma(\mathbb{C}_\infty)$ et soit $\mathfrak{p} = (P)$ un idéal premier de A tel que $P \equiv 1 \bmod n$. Par un analogue du théorème de Dirichlet ([37, Theorem 4.7]), un tel polynôme P existe. On a

$$T_\mathfrak{p} u_\varphi(z) = u_\varphi(Pz) \prod_{\substack{j \in A \\ \deg(j) < \deg(P)}} u_\varphi\left(\frac{z+j}{P}\right).$$

Puisque $T_{\mathfrak{p}}$, comme tout autre opérateur Hecke, commute avec l'application $f \in \mathrm{Hom}(\overline{\Gamma}, \mathbb{C}_\infty) \mapsto f(\varphi) \in \mathbb{C}_\infty^*$, on a par (2.20),

$$u_\varphi(z)^{\lambda_{\mathfrak{p}}} = u_\varphi(Pz) \prod_{\substack{j \in A \\ \deg(j) < \deg(P)}} u_\varphi\left(\frac{z+j}{P}\right). \tag{2.24}$$

Soit $s \in \Gamma\backslash\mathbb{P}^1(K)$ une pointe. On pose $\mathcal{S}_P = \{j \in A,\ \deg(j) < \deg(P)\}$. Puisque $P \equiv 1 \bmod n$ et par des arguments similaires à [11, Proposition 2.2.3], il existe des matrices Q_P et $(Q_j)_{j \in \mathcal{S}_\mathcal{P}} \subset \Gamma$ tels que $Q_P s = Ps$ et $Q_j s = \dfrac{s+j}{P}$ pour tout $j \in \mathcal{S}_P$. On prend $z = s$ dans (2.24), et en divisant par $u_\varphi(s)^{q^{\deg(P)+1}}$, on obtient

$$\begin{aligned} u_\varphi(s)^{\lambda_{\mathfrak{p}} - (q^{\deg(P)}+1)} &= \frac{u_\varphi(Ps)}{u_\varphi(s)} \prod_{\substack{j \in A \\ \deg(j) < \deg(P)}} \frac{u_\varphi\left(\frac{s+j}{P}\right)}{u_\varphi(s)}, \\ &= \underbrace{\frac{u_\varphi(Q_P s)}{u_\varphi(s)} \prod_{\substack{j \in A \\ \deg(j) < \deg(P)}} \frac{u_\varphi(Q_j s)}{u_\varphi(s)}}_{\in \Lambda}. \end{aligned}$$

Donc $\Phi(s)$ est un point de torsion de $E(K_\infty)$ dont l'ordre divise $\#(\overline{E}(\mathbb{F}_{\mathfrak{p}}))$. □

Remarque. Dans des cas spécifiques, des bornes explicites pour la taille du sous-groupe cuspidal de la jacobienne sont connues, par exemple lorsque n est irréductible par Gekeler ([19]) ou $\deg(n) = 3$ par Papikian et Wei ([34]). Ces bornes qui, contrairement au théorème 99, ne dépendent que de n, sont également des bornes supérieures pour l'ordre des points de torsion sur la courbe elliptique provenant de l'évaluation de Φ aux pointes. Cependant le théorème 99 ne requiert aucune hypothèse sur n.

2.7 Exemple sur $\mathbb{F}_2(T)$ avec $n = T^3$

On considère la courbe elliptique $E/\mathbb{F}_2(T)$ définie par

$$y^2 + Txy = x^3 + T^2.$$

Son conducteur est $\mathfrak{n} = T^3\infty$. La courbe elliptique E est isomorphe sur $\mathbb{F}_2(T)$ à la courbe de Weil forte donnée dans [38, Theorem 2.1 (a)]. On pose $n = T^3$

et $\Gamma = \Gamma_0(n)$. Le genre de $\overline{M}_\Gamma$ est 1, donc le groupe abélien $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ est de rang 1.

Soit $\varphi_E \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ la cochaîne harmonique associée à E comme décrite dans la section 2.6. On peut identifier φ_E à l'aide de son développement en série de Fourier : en effet puisque φ_E possède un support fini modulo Γ, il suffit de connaître ses valeurs sur les arêtes de $(\Gamma\backslash\mathcal{T})^0$ qui sont en nombre fini. L'arbre quotient a été calculé dans l'exemple 59. De plus, on peut calculer l'image réciproque de φ_E par l'isomorphisme j du théorème 69. Pour ce faire, on calcule l'image réciproque d'une $\mathbb{Z}$-base de $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ avec la méthode du sous-arbre maximal de $\Gamma\backslash\mathcal{T}$ comme fait dans [26, preuve du Lemme 3.3.3] et rappelé dans le lemme 68. Ici comme $\mathrm{rg}(\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma) = 1$, la cochaîne φ vérifiant $\varphi(\tilde{e}_{01}) = 1$ est un générateur de $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$. On cherche maintenant $\gamma \in \Gamma$ telle que $j(\gamma) = \varphi$. Pour ce faire, on considère l'unique géodésique $\tilde{c}$ reliant $\tilde{v}_{01} = o(\tilde{e}_{01})$ à $\tilde{v}_{11} = t(\tilde{e}_{01})$ dans $\Gamma\backslash\mathcal{T} - \{\tilde{e}_{01}\}$, puis on prend une géodésique dans $\mathcal{T}$ qui est un relèvement de $\{\tilde{e}_{01}\}\cup\tilde{c}$. La géodésique suivante est un relèvement de $\{\tilde{e}_{01}\}\cup\tilde{c}$:

$$v(2,\pi) \in \tilde{v}_{01} \to v(1,0) \to v(2,0) \to v(3,\pi^2) \to v(4,\pi^3+\pi^2).$$

Notons $v = v(2,\pi)$ et $v' = v(3,\pi^2)$. Il suffit de déterminer $\gamma \in \Gamma$ telle que $v' = \gamma v$. On obtient

$$\gamma = \begin{pmatrix} T+1 & 1 \\ T^3 & T^2+T+1 \end{pmatrix}.$$

L'application φ_E vérifie $\varphi_E(\tilde{e}_{01}) = -1$. On en déduit que l'image réciproque de φ_E par j est la matrice

$$\alpha = \begin{pmatrix} 1+T+T^2 & 1 \\ T^3 & 1+T \end{pmatrix} \in \Gamma.$$

On remarque que α engendre $\overline{\Gamma}$ puisque φ_E engendre $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$, donc

$$\Lambda = \{c_\alpha(\gamma), \gamma \in \overline{\Gamma}\} = \langle c_\alpha(\alpha)\rangle.$$

Pour déterminer le réseau Λ, il suffit de calculer $c_\alpha(\alpha)$. Le coefficient multiplicateur $c_\alpha(\alpha)$ est donné par (voir (2.13))

$$c_\alpha(\alpha) = \prod_{\gamma\in\widetilde{\Gamma}} \frac{\alpha\infty - \gamma\omega}{\alpha\infty - \gamma\alpha\omega}, \tag{2.25}$$

et ce produit est indépendant de $\omega \in \Omega$. On choisit $\omega = T^{-2}\rho$ avec $\rho \in \mathbb{C}_\infty^*$ satisfaisant $\rho^2+\rho+1 = 0$. On obtient l'approximation de $c_\alpha(\alpha)$ suivante en

restreignant le produit (2.25) à l'ensemble

$$\left\{\gamma \in \widetilde{\Gamma}, \left|\frac{\alpha\infty - \gamma\omega}{\alpha\infty - \gamma\alpha\omega} - 1\right| \geq \frac{1}{16}\right\}.$$

Cet ensemble est alors déterminé par des arguments similaires à ceux de la preuve de la proposition 100. On obtient $c_\alpha(\alpha) = \pi^{-4} + \delta_{c_\alpha(\alpha)}$ où $\delta_{c_\alpha(\alpha)} \in K_\infty^*$ est tel que $|\delta_{c_\alpha(\alpha)}| < 1$. On en déduit qu'un générateur de Λ est

$$t = c_\alpha(\alpha)^{-1} = \pi^4 + \delta_{t_\alpha},$$

avec $|\delta_{t_\alpha}| < 2^{-8}$.
La courbe modulaire $\overline{M}_\Gamma$ possède 4 pointes : $\infty, 0, \frac{1}{T}, \frac{1}{T^2}$. Par le théorème 98, le degré de la paramétrisation modulaire est 1 et Φ est donc un isomorphisme. Pour une pointe $c \in \{\infty, 0, \frac{1}{T}, \frac{1}{T^2}\}$, on veut évaluer $u_\alpha(c)$ modulo Λ. En utilisant le théorème 99, on calcule $\#(\overline{E}(\mathbb{F}_\mathfrak{p}))$ pour tout premier $\mathfrak{p} = (P)$ vérifiant $\deg(P) \leq 15$: on obtient que l'image de c est un point de torsion dans E d'ordre divisant 16. Noter que dans cet exemple, la borne donnée par Papikian-Wei dans [34] est 4, ce qui est meilleur que la nôtre.

Proposition 100. *On a les approximations suivantes :*

$$\begin{aligned}
&u_\alpha(0) = \pi + \upsilon, && \text{avec } |\upsilon| < 2^{-5},\\
&u_\alpha\left(\frac{1}{T}\right) = \pi^{-1} + \delta_{1/T}, && \text{avec } |\delta_{1/T}| < 2^{-3},\\
&u_\alpha\left(\frac{1}{T^2}\right) = \pi^2 + \delta_{1/T^2}, && \text{avec } |\delta_{1/T^2}| < 2^{-6}.
\end{aligned}$$

En particulier, les points $\Phi(0)$ et $\Phi(\frac{1}{T})$ sont d'ordre 4 dans $E(K_\infty)$, et le point $\Phi(\frac{1}{T^2})$ est d'ordre 2 dans $E(K_\infty)$.

Démonstration. Nous ne détaillons que le calcul de u_α en $s = 0$. Rappelons que par le théorème 85, la valeur $u_\alpha(0)$ est donnée par

$$u_\alpha(0) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{0 - \gamma\omega}{0 - \gamma\alpha\omega}.$$

Comme précédemment, on choisit $\omega = T^{-2}\rho$ avec $\rho^2 + \rho + 1 = 0$. On observe alors que $|\omega| = |\omega|_i = 2^{-2}$, $|\alpha\omega| = 2^{-1}$ et $|\alpha\omega|_i = 2^{-4}$. Pour $z \in \overline{\Omega}$, on note $G_{\gamma,\omega}(z) = \dfrac{z - \alpha\omega}{z - \gamma\alpha\omega}$. En premier lieu, on a besoin de majorer les normes des produits partiels. On remarque que si $\sup\limits_{\mathcal{S} \subset \Gamma} \left|\prod\limits_{\gamma \in \mathcal{S}} G_{\gamma,\omega}(0)\right| = C$ et si

$$\widetilde{\Gamma}_\varepsilon = \{\gamma \in \widetilde{\Gamma}, |G_{\gamma,\omega}(0) - 1| \geq \varepsilon\},$$

alors on a

$$\begin{aligned}\left|\prod_{\gamma\in\widetilde{\Gamma}} G_{\gamma,\omega}(0) - \prod_{\gamma\in\widetilde{\Gamma}_\varepsilon} G_{\gamma,\omega}(0)\right| &= \underbrace{\left|\prod_{\gamma\in\widetilde{\Gamma}_\varepsilon} G_{\gamma,\omega}(0)\right|}_{\leq C}\left|\prod_{\gamma\in\widetilde{\Gamma}-\widetilde{\Gamma}_\varepsilon} G_{\gamma,\omega}(0) - 1\right| \\ &\leq C\left|\prod_{\gamma\in\widetilde{\Gamma}-\widetilde{\Gamma}_\varepsilon} 1 + (G_{\gamma,\omega}(0)-1)\right| \\ &\leq C\left|\sum_{j=1}^{\infty}\sum_{\substack{\Upsilon\subset\widetilde{\Gamma}-\widetilde{\Gamma}_\varepsilon \\ \#\Upsilon=j}}\prod_{\gamma\in\Upsilon}\underbrace{(G_{\gamma,\omega}(0)-1)}_{\leq\varepsilon}\right| \\ &\leq C\max_{j\geq 1}\max_{\substack{\Upsilon\subset\widetilde{\Gamma}-\widetilde{\Gamma}_\varepsilon \\ \#\Upsilon=j}}\varepsilon^j \\ &\leq C\varepsilon.\end{aligned}$$

Commençons donc par majorer le supremum des normes des produits partiels. Soit $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$ un élément de $\widetilde{\Gamma}$. On a

$$\left|\frac{-\gamma\omega}{-\gamma\alpha\omega}\right| = \left|1 + \frac{\gamma\alpha\omega-\gamma\omega}{-\gamma\alpha\omega}\right| \leq \max\left(1, \left|\frac{\gamma\alpha\omega-\gamma\omega}{-\gamma\alpha\omega}\right|\right),$$

et par (2.15),

$$\left|\frac{\gamma\alpha\omega-\gamma\omega}{-\gamma\alpha\omega}\right| = \frac{|\alpha\omega-\omega|}{|-\gamma\alpha\omega||c\omega+d||c\alpha\omega+d|} = \frac{2^{-1}}{|a\alpha\omega+b||c\omega+d|}. \tag{2.26}$$

Mais on a

$$\begin{aligned}|a\alpha\omega+b| &= \frac{|(a(1+T+T^2)+bT^3)\omega+b(1+T)+a|}{|T^3\omega+1+T|} \\ &\geq 2^{-1}\left|(a(1+T+T^2)+bT^3)\omega+b(1+T)+a\right| \\ &\geq 2^{-1}.\end{aligned}$$

Ainsi si $c\neq 0$

$$\left|\frac{\gamma\alpha\omega-\gamma\omega}{-\gamma\alpha\omega}\right| \leq \frac{1}{|c\omega+d|} \leq \frac{2^2}{|c|} \leq 2^{-1}.$$

Si $c = 0$, alors $a = d = 1$ et $|c\omega + d| = 1$, puis on a

$$\left|\frac{\gamma\alpha\omega - \gamma\omega}{-\gamma\alpha\omega}\right| = \frac{2^{-1}}{|\alpha\omega + b|} \leq 1.$$

Pour tout sous-ensemble $\mathcal{S} \subset \widetilde{\Gamma}$, on déduit que

$$\left|\prod_{\gamma\in\mathcal{S}} \frac{-\gamma\omega}{-\gamma\alpha\omega}\right| \leq 1. \tag{2.27}$$

Par cette inégalité, on voit que pour calculer $u_\alpha(0)$ avec une précision au plus ε, il suffit de calculer le produit

$$\prod_{\substack{\gamma\in\widetilde{\Gamma}\\ |G_{\gamma,\omega}(0)-1|\geq\varepsilon}} G_{\gamma,\omega}(0),$$

où $G_{\gamma,\omega}(z) = \dfrac{z - \gamma\omega}{z - \gamma\alpha\omega}$. Lorsque $|c| > \frac{2^2}{\varepsilon}$, on a

$$\begin{aligned} |G_{\gamma,\omega}(0) - 1| &= \frac{2^{-1}}{|a\alpha\omega + b||c\omega + d|} \qquad \text{(par (2.26))} \\ &\leq \frac{2^2}{|c|} < \varepsilon. \end{aligned}$$

Si $|c| \leq \frac{2^2}{\varepsilon}$ et $|d| > \frac{2}{\varepsilon}$, on obtient que $|G_{\gamma,\omega}(0) - 1| < \varepsilon$. Maintenant pour les couples (c, d) ne vérifiant pas la condition ($|c| > \frac{2^2}{\varepsilon}$ ou $|d| > \frac{2}{\varepsilon}$) alors, si $c \neq 0$ on a $|c\omega + d| \geq |c||\omega|_i \geq 2^1$, et alors

$$|G_{\gamma,\omega}(0) - 1| \leq \frac{2^{-2}}{|a\alpha\omega + b|} < \frac{2^2}{|a|} < \varepsilon \qquad \text{si } |a| > \frac{2^2}{\varepsilon}.$$

Lorsque $c = 0$ (ce qui implique $a = d = 1$), alors si $|b| > \frac{2^{-1}}{\varepsilon}$, on obtient

$$|G_{\gamma,\omega}(0) - 1| = \frac{2^{-1}}{|\alpha\omega + b|} \leq \frac{2^{-1}}{|b|} < \varepsilon.$$

On note qu'à l'exception du cas $c = 0$, pour a, c, d fixés, il existe au plus une valeur de $b \in A$ tel que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Donc, pour approcher $u_\alpha(0)$ à la précision au plus ε nous devons calculer le produit

$$\prod_{\gamma\in\widetilde{\Gamma}_\varepsilon} G_{\gamma,\omega}(0),$$

où $\widetilde{\Gamma}_\varepsilon = \widetilde{\Gamma}_\varepsilon^c \cup \widetilde{\Gamma}_\varepsilon^0$ avec

$$\widetilde{\Gamma}_\varepsilon^c = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}, c \neq 0, |c| \leq \frac{2^2}{\varepsilon}, |d| \leq \frac{2}{\varepsilon}, |a| \leq \frac{2^2}{\varepsilon} \right\},$$

et

$$\widetilde{\Gamma}_\varepsilon^0 = \left\{ \gamma \in \widetilde{\Gamma}, c = 0, |b| \leq \frac{1}{2\varepsilon} \right\}.$$

Le calcul du produit fini $\prod_{\gamma \in \widetilde{\Gamma}_\varepsilon} G_{\gamma,\omega}(0)$ pour $\varepsilon = 2^{-5}$ a été effectué avec le logiciel PARI/GP [48]. On obtient $u_\alpha(0) = \pi + \upsilon$ avec $\upsilon \in K_\infty^*$ vérifiant $|\upsilon| < 2^{-5}$, donc $u_\alpha(0)^4 = t + \upsilon^4$. On conclut que $\Phi(0)$ est d'ordre 4.

Pour $s = \frac{1}{T}$, on obtient $u_\alpha(\frac{1}{T}) = \pi^{-1} + \delta_{1/T}$ avec $\delta_{1/T} \in K_\infty^*$ satisfaisant $|\delta_{1/T}| < 2^{-3}$: on en déduit que le point $\Phi(1/T)$ est d'ordre 4 sur E. Finalement, on a $u_\alpha\left(\frac{1}{T^2}\right) = \pi^2 + \delta_{1/T^2}$ avec $|\delta_{1/T^2}| \leq 2^{-6}$, donc le point $\Phi\left(\frac{1}{T^2}\right)$ est d'ordre 2. □

Remarque. Dans cet exemple, nous pouvons également donner une borne explicite sur le cardinal de l'ensemble $\widetilde{\Gamma}_\varepsilon$. L'ensemble

$$S = \{c \in \mathbb{F}_2[T] : c \equiv 0 \bmod T^3, \deg(c) \leq 2 + \lfloor \log_2(\frac{1}{\varepsilon}) \rfloor\}$$

est de cardinal l $2^{-\lfloor \log_2(\varepsilon) \rfloor}$. Soit $c \in S$. On considère l'ensemble S_c des polynômes $d \in \mathbb{F}_2[T]$ tels qu'il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}$: une majoration de son cardinal est

$$\#(\{d \in \mathbb{F}_2[T] : \deg(d) \leq 1 - \lfloor \log_2(\varepsilon) \rfloor, \operatorname{pgcd}(d, T) = 1\}) = 2^{2 - \lfloor \log_2(\varepsilon) \rfloor}.$$

Alors pour $c \in S$ et $d \in S_c$, le nombre de polynômes possibles a tels qu'il existe $b \in A$ satisfaisant $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}$ est majoré par

$$\#(\{a \in \mathbb{F}_2[T], \operatorname{pgcd}(a, T) = 1 \text{ et } \deg(a) \leq 2 - \log_2(\varepsilon)\}) = 2^{2 - \lfloor \log_2(\varepsilon) \rfloor}.$$

Alors on obtient $\#(\widetilde{\Gamma}_\varepsilon) \leq 2^{4 - 3\lfloor \log_2(\varepsilon) \rfloor}$.

2.8 Exemple sur $\mathbb{F}_3(T)$ avec $n = T^3 - T^2$

On considère la courbe elliptique $E/\mathbb{F}_3(T)$ définie par

$$E\colon y^2 = x^3 + T(T+1)x^2 + T^2 x.$$

Son conducteur est $\infty(T^3 - T^2)$ et son j-invariant est

$$j_E = \frac{(T^2+T+1)^3}{T(T+1)}.$$

De nouveau E est une courbe de Weil forte, voir [38, Théorème 2.4 (b)]. Soit $n = T^3 - T^2$ la partie finie du conducteur de E et soit $\Gamma = \Gamma_0(T^3 - T^2)$. Ici le genre de la courbe $\overline{M}_\Gamma$ est 2 et donc le groupe abélien $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ est de rang 2. On a besoin de connaître l'arbre quotient déjà calculé dans l'exemple 60. On reprend les mêmes notations que dans cet exemple. Soit $\varphi_1 \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$, la cochaîne harmonique vérifiant

$$\varphi_1(\tilde{e}) = \begin{cases} n(\tilde{e}) & \text{si } \tilde{e} \in \tilde{c}_1 \\ -n(\tilde{e}) & \text{si } \overline{\tilde{e}} \in \tilde{c}_1, \\ 0 & \text{sinon} \end{cases}$$

où $\tilde{c}_1 = \tilde{g}(\tilde{v}_{11}, \tilde{v}_{01}) \cup \{\tilde{e}_{02}\}$, où $\tilde{g}(\tilde{v}_{11}, \tilde{v}_{01})$ est l'unique géodésique allant de $\tilde{v}_{11}$ à $\tilde{v}_{01}$ dans le sous-arbre maximal $\Gamma\backslash\mathcal{T} - \{\tilde{e}_{02}, \tilde{e}_{04}\}$ Il suffit de prendre un relèvement de $\tilde{c}_1$ dans $\mathcal{T}$:

$$v(2,\pi) \to v(3, 2\pi^2+\pi) \to v(5, \pi^4+\pi^3+2\pi^2+\pi) \to v(6, \pi^4+\pi^3+2\pi^2+\pi).$$

On en déduit $j^{-1}(\varphi_1) = \begin{pmatrix} T^2+T+2 & 2 \\ T^3+2T^2 & 2T+2 \end{pmatrix}$. On fait de même pour $\tilde{c}_2 = \tilde{g}(\tilde{v}_{14}, \tilde{v}_{01}) \cup \{\tilde{e}_{04}\}$:

$$\begin{array}{l} v(2,\pi^2) \longrightarrow v(3, 2\pi^2+\pi) \longrightarrow v(4, 2\pi^2+\pi) \longrightarrow v(5, \pi^4+2\pi^2+\pi) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad v(6, \pi^5+\pi^4+2\pi^2+\pi), \end{array}$$

et on en déduit que $j^{-1}(\varphi_2) = \begin{pmatrix} T^3+T^2+T+1 & 2T^2+T+1 \\ T^4+2T^3 & 2T^3+T+2 \end{pmatrix}$.

Soit φ_E la forme automorphe associée à E. À l'aide du développement en série de Fourier de φ_E, on obtient que $\varphi_E = \varphi_1 - \varphi_2$. L'image réciproque de φ_E par l'isomorphisme j est

$$j^{-1}(\varphi_E) = j^{-1}(\varphi_1) j^{-1}(\varphi_2)^{-1} = \begin{pmatrix} T^3+2T^2+2T+2 & 2T+1 \\ T^4+T^3+T^2 & 2T^2+2T+1 \end{pmatrix}.$$

On calcule un générateur $t \in K_\infty^*$ du réseau $\Lambda = \{c_\alpha(\gamma), \gamma \in \widetilde{\Gamma}\} = t^{\mathbb{Z}}$. On obtient l'approximation suivante pour t :

$$t = \pi^4 + 2\pi^5 + O(\pi^6).$$

La courbe modulaire $\overline{M}_\Gamma$ possède six pointes : $\infty, 0, \frac{1}{T}, \frac{1}{T^2}, \frac{1}{T-1}, \frac{1}{T^2-T}$. La période de Tate de E est donnée par (voir [45, Section 2 de l'Annexe A])

$$t_E = \sum_{n\geq 1} d(n)\frac{1}{j_E^n} = \pi^4 + 2\pi^5 + \pi^7 + 2\pi^8 + \delta_{t_E},$$

où $(d(n))_{n\geq 1}$ sont les coefficients de la série pour la fonction réciproque de j, et $\delta_{t_E} \in K_\infty^*$ satisfait $|\delta_{t_E}| < 3^{-10}$. On en déduit que $t_E = t$. Le degré de la paramétrisation modulaire est 2. Comme précédemment, on calcule $\#(\overline{E}(\mathbb{F}_\mathfrak{p}))$ pour les idéaux premiers $\mathfrak{p} = (P)$ tels que $\deg(P) \leq 10$ et $P \equiv 1 \bmod n$. Par le théorème 99, on obtient que l'ordre de l'image d'une pointe divise 8. Cette borne est meilleure que celle déduite de Papikian-Wei [34] qui est 24 dans cet exemple.

Proposition 101. *On a les approximations suivantes :*

$$\begin{aligned}
&u_\alpha(0) = 2\pi^2 + 2\pi^3 + \vartheta_0, && \text{avec } |\vartheta_0| < 3^{-3},\\
&u_\alpha\left(\frac{1}{T}\right) = \pi^{-1} + 1 + \pi + \vartheta_{1/T}, && \text{avec } |\vartheta_{1/T}| < 3^{-1},\\
&u_\alpha\left(\frac{1}{T^2}\right) = \pi^4 + 2\pi^5 + \vartheta_{1/T^2} && \text{avec } |\vartheta_{1/T^2}| < 3^{-5},\\
&u_\alpha\left(\frac{1}{T-1}\right) = \pi^{-2} + \pi^{-1} + \vartheta_{1/(T-1)}, && \text{avec } |\vartheta_{1/(T-1)}| < 1,\\
&u_\alpha\left(\frac{1}{T^2-T}\right) = \pi^3 + \vartheta_{1/(T^2-T)}, && \text{avec } |\vartheta_{1/(T^2-T)}| < 3^{-5}.
\end{aligned}$$

En particulier, on obtient

1. *Les points* $\Phi\left(\frac{1}{T}\right)$ *et* $\Phi\left(\frac{1}{T^2-T}\right)$ *sont d'ordre* 4 *sur* $E(K_\infty)$.
2. *Le point* $\Phi\left(\frac{1}{T^2}\right)$ *est d'ordre* 1 *sur* $E(K_\infty)$.
3. *Les points* $\Phi(0)$ *et* $\Phi\left(\frac{1}{T-1}\right)$ *sont d'ordre* 2 *sur* $E(K_\infty)$.

Démonstration. Comme précédemment, pour $s \in \Gamma\backslash\mathbb{P}^1(K)$ et $\gamma \in \Gamma$, on pose $G_{\gamma,\omega}(s) = \dfrac{s-\gamma\omega}{s-\gamma\alpha\omega}$. Comme système de représentants pour $\tilde{\Gamma}$, on choisit les matrices de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ avec a unitaire. Pour $\varepsilon \leq 1$, soit

$$\mathcal{S}_\varepsilon = \{\gamma \in \widetilde{\Gamma}, |G_{\gamma,\omega}(s) - 1| \geq \varepsilon\}.$$

On a $\left|\prod_{\gamma\in\mathcal{S}_\varepsilon} G_{\gamma,\omega}(s)\right| \leq \left|\prod_{\gamma\in\mathcal{S}_1} G_{\gamma,\omega}(s)\right|$ et

$$\left|\prod_{\gamma\in\widetilde{\Gamma}} G_{\gamma,\omega}(s) - \prod_{\gamma\in\mathcal{S}_\varepsilon} G_{\gamma,\omega}(s)\right| < \left|\prod_{\gamma\in\mathcal{S}_1} G_{\gamma,\omega}(s)\right| \varepsilon.$$

En effet, en posant $g_{\gamma,\omega}(s) = G_{\gamma,\omega}(s) - 1$, on a

$$\left|\prod_{\gamma\in\widetilde{\Gamma}-\mathcal{S}_\varepsilon} G_{\gamma,\omega}(s) - 1\right| = \left|\prod_{\gamma\in\widetilde{\Gamma}-\mathcal{S}_\varepsilon} (1 + g_{\gamma,\omega}(s)) - 1\right|$$

et on voit facilement que $\prod_{\gamma\in\widetilde{\Gamma}-\mathcal{S}_\varepsilon} (1 + g_{\gamma,\omega}(s)) = 1 + \delta_{\omega,\varepsilon}(s)$ avec $|\delta_{\omega,\varepsilon}(s)| < \varepsilon$.

Nous donnons des détails uniquement pour la pointe $s = \frac{1}{T}$. On choisit $\omega = T^{-2}\rho$ avec $\rho^2 + 1 = 0$. On remarque que $|\omega| = |\omega|_i = 3^{-2}$, $|\alpha\omega| = 3^{-1}$ et $|\alpha\omega|_i = 3^{-4}$. Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. On a

$$|s - \gamma\alpha\omega| = \frac{|(c - aT)\alpha\omega + (d - bT)|}{|T||c\alpha\omega + d|}.$$

De plus, on a

$$|(c - aT)\alpha\omega + d - bT| \geq 3^{-2}.$$

On obtient alors par (2.15) que si $|c| > \frac{3^4}{\varepsilon}$

$$|G_{\gamma,\omega}(s) - 1| \leq \frac{3^3|\alpha\omega - \omega|}{|c\omega + d|} \leq \frac{3^2}{|c||\omega|_i} \leq \frac{3^4}{|c|} < \varepsilon.$$

D'autre part, si $|c| \leq \frac{3^4}{\varepsilon}$ et $|d| > \frac{3^2}{\varepsilon}$, il vient que $|c\omega + d| = |d|$ et l'on obtient

$$|G_{\gamma(s),\omega} - 1| = \frac{3^2}{|d|} < \varepsilon.$$

Si (c, d) ne satisfait pas la condition ($|c| > \frac{3^4}{\varepsilon}$ ou $|d| > \frac{3^2}{\varepsilon}$) et si $c \neq 0$, on remarque que si $|a| > \frac{3^5}{\varepsilon}$, on a $|a\alpha\omega + b| > |c\alpha\omega + d||s|$. On obtient donc

$$|s - \gamma\alpha\omega| = \left|s - \frac{a\alpha\omega + b}{c\alpha\omega + d}\right| = \frac{|a\alpha\omega + b|}{|c\alpha\omega + d|}.$$

Puisque $|c\omega+d| \geq |c||\omega|_i \geq 3^1$, On obtient par (2.15)

$$|G_{\gamma,\omega}(s)-1| \leq \frac{|\alpha\omega-\omega|}{|a\alpha\omega+b||c\omega+d|} \leq \frac{3^2}{|a|} < \varepsilon, \qquad \text{si } |a| > \frac{3^5}{\varepsilon}.$$

Lorsque $c=0$, on a $a=1$ et $d \in \mathbb{F}_3^*$, et l'on obtient pour $b \neq 0$:

$$|s-\gamma\alpha\omega| = |s-\frac{\alpha\omega}{d}-\frac{b}{d}| = |b|.$$

Donc

$$|G_{\gamma,\omega}(s)-1| = \frac{|\alpha\omega-\omega|}{|b||c\omega+d|} \leq \frac{3^{-2}}{|b|} < \varepsilon, \qquad \text{si } |b| > \frac{3^{-2}}{\varepsilon}.$$

Ici le produit $\prod_{\gamma\in\mathcal{S}_1} G_{\gamma,\omega}(s)$ est de norme 3. Donc, si nous voulons approcher le produit $\prod_{\gamma\in\widetilde{\Gamma}} G_{\gamma,\omega}(s)$ à la précision au plus ε, il faut considérer le produit restreint à l'ensemble $\mathcal{S}_{\varepsilon/3}$.

Pour $\varepsilon = 3^{-1}$, le calcul de $u_\alpha\left(\frac{1}{T}\right)$ à la précision au plus 3^{-1} donne $u_\alpha\left(\frac{1}{T}\right) = \pi^{-1}+1+\pi+\vartheta_{1/T}$, avec $\vartheta_{1/T} \in K_\infty^*$ satisfaisant $|\vartheta_{1/T}| < 3^{-1}$. Pour les autres pointes, on obtient

$$\begin{aligned}
&u_\alpha(0) = 2\pi^2+2\pi^3+\vartheta_0, && \text{avec } |\vartheta_0| < 3^{-3},\\
&u_\alpha\left(\frac{1}{T^2}\right) = \pi^4+2\pi^5+\vartheta_{1/T^2} && \text{avec } |\vartheta_{1/T^2}| < 3^{-5},\\
&u_\alpha\left(\frac{1}{T-1}\right) = \pi^{-2}+\pi^{-1}+\vartheta_{1/(T-1)}, && \text{avec } |\vartheta_{1/(T-1)}| < 1,\\
&u_\alpha\left(\frac{1}{T^2-T}\right) = \pi^3+\vartheta_{1/(T^2-T)}, && \text{avec } |\vartheta_{1/(T^2-T)}| < 3^{-5}.
\end{aligned}$$

Cela prouve le résultat. □

Remarque. Nous pouvons également majorer le cardinal de l'ensemble $\mathcal{S}_{1/9}$ nécessaire pour calculer $u_\alpha\left(\frac{1}{T}\right)$ à la précision au plus $\varepsilon = 3^{-1}$. On a

$$\#(\{c \in \mathbb{F}_3[T], \deg(c) \leq 7 \text{ et } (T^3-T^2) \mid c\}) = 3^4,$$
$$\#\left(\{d \in \mathbb{F}_3[T], \deg(d) \leq 4 \text{ et } \operatorname{pgcd}(d, T^3-T^2) \in \mathbb{F}_3^*\}\right) \leq 3^4.$$

Ainsi le nombre de couples (c,d) tels que (c,d) peut être relevé en une matrice de $\widetilde{\Gamma}$ est majoré par 3^8. On a également

$$\#\left(\{a \in \mathbb{F}_3[T],\ \deg(a) \leq 7,\ a \text{ unitaire et } \operatorname{pgcd}(a, T^3-T^2) \in \mathbb{F}_3^*\}\right) \leq 3^7.$$

On en conclut que $\#(\mathcal{S}_{1/9}) \leq 3^{15}$.

Bibliographie

[1] Ayad, M. (1992). Points S-entiers des courbes elliptiques. *Manuscripta mathematica*, 76(1) :305–324.

[2] Bermudez Tobon, Y. (2015). *An efficient algorithm to compute an elliptic curve from a corresponding function field automorphic form.* PhD thesis, Heidelberg University.

[3] Bettin, S., David, C., and Delaunay, C. (2018). Non-isotrivial elliptic surfaces with non-zero average root number. *Journal of Number Theory*, 191 :1–84.

[4] Breuil, C., Conrad, B., Diamond, F., and Taylor, R. (2001). On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939.

[5] Brunault, F. (2016). On the ramification of modular parametrizations at the cusps. *Journal de Théorie des Nombres de Bordeaux*, 28(3) :773–790.

[6] Butenuth, R. (2012). *Quaternionic Drinfeld modular forms.* PhD thesis, Heidelberg University.

[7] Chen, H. (2016). Computing the Mazur and Swinnerton-Dyer critical subgroup of elliptic curves. *Mathematics of Computation*, 85(301) :2499–2514.

[8] Cohen, H. (1993). *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin.

[9] Cohen, H. (2007). *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics.* Springer, New York.

[10] Cremona, J. (1995). Computing the degree of the modular parametrization of a modular elliptic curve. *Mathematics of computation*, 64(211) :1235–1250.

[11] Cremona, J. E. (1997). *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition.

[12] Delaunay, C. (2003). Computing modular degrees using L-functions. *Journal de théorie des nombres de Bordeaux*, 15(3) :673–682.

[13] Delaunay, C. (2005). Critical and ramification points of the modular parametrization of an elliptic curve. *Journal de théorie des nombres de Bordeaux*, 17(1) :109–124.

[14] Delaunay, C. and Duquesne, S. (2003). Numerical investigations related to the derivatives of the L-series of certain elliptic curves. *Experimental mathematics*, 12(3) :311–317.

[15] Drinfel'd, V. G. (1974). Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4) :561.

[16] Duquesne, S. (2001). Integral points on elliptic curves defined by simplest cubic fields. *Experimental Mathematics*, 10(1) :91–102.

[17] Gekeler, E.-U. (1985). Automorphe Formen über $\mathbf{F}_q(T)$ mit kleinem Führer. *Abh. Math. Sem. Univ. Hamburg*, 55 :111–146.

[18] Gekeler, E.-U. (1986a). *Drinfeld modular curves*, volume 1231 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin.

[19] Gekeler, E.-U. (1986b). Über Drinfeldsche Modulkurven vom Hecke-Typ. *Compositio Math.*, 57(2) :219–236.

[20] Gekeler, E.-U. (1995a). Analytical construction of Weil curves over function fields. *Journal de théorie des nombres de Bordeaux*, 7(1) :27–49.

[21] Gekeler, E.-U. (1995b). Improper Eisenstein series on Bruhat-Tits trees. *manuscripta mathematica*, 86(1) :367–391.

[22] Gekeler, E.-U. (1997a). Jacquet-Langlands theory over K and relations with elliptic curves. In *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 224–257. World Sci. Publ., River Edge, NJ.

[23] Gekeler, E.-U. (1997b). On the cuspidal divisor class group of a Drinfeld modular curve. *Doc. Math.*, 2 :351–374.

[24] Gekeler, E.-U. (2000). A note on the finiteness of certain cuspidal divisor class groups. *Israel Journal of Mathematics*, 118(1) :357–368.

[25] Gekeler, E.-U. and Nonnengardt, U. (1995). Fundamental domains of some arithmetic groups over function fields. *International Journal of Mathematics*, 6(5) :689–708.

[26] Gekeler, E.-U. and Reversat, M. (1996). Jacobians of Drinfeld modular curves. *J. Reine Angew. Math.*, 476 :27–93.

[27] Goss, D. (1996). *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin.

[28] Hindry, M. and Silverman, J. H. (2000). *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York. An introduction.

[29] Jacquet, H. and Langlands, R. P. (1970). *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York.

[30] Krir, M. (2001). À propos de la conjecture de Lang sur la minoration de la hauteur de Néron-Tate pour les courbes elliptiques sur $\mathbf{Q}$. *Acta Arith.*, 100(1) :1–16.

[31] Mazur, B. (1977). Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47) :33–186 (1978). With an appendix by Mazur and M. Rapoport.

[32] Mazur, B. and Swinnerton-Dyer, P. (1974). Arithmetic of Weil curves. *Invent. Math.*, 25 :1–61.

[33] Néron, A. (1952). Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. *Bull. Soc. Math. France*, 80 :101–166.

[34] Papikian, M. and Wei, F.-T. (2016). On the Eisenstein ideal over function fields. *Journal of Number Theory*, 161 :384–434.

[35] Petit, V. (2022a). Explicit computation of the modular parametrization of elliptic curves over function fields by Drinfeld modular curves. *arXiv preprint arXiv :2206.00896*.

[36] Petit, V. (2022b). Non-divisible point on a two-parameter family of elliptic curves. *Res. Number Theory*, 8(1) :Paper No. 6, 16.

[37] Rosen, M. (2002). *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[38] Schweizer, A. (2011). Strong Weil curves over $\mathbb{F}_q(T)$ with small conductor. *J. Number Theory*, 131(2) :285–299.

[39] Serre, J.-P. (2003). *Trees*. Springer Monographs in Mathematics. Springer-Verlag, Berlin. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.

[40] Silverman, J. H. (1983). Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342 :197–211.

[41] Silverman, J. H. (1985). Divisibility of the specialization map for families of elliptic curves. *American Journal of Mathematics*, 107(3) :555–565.

[42] Silverman, J. H. (1986). *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[43] Silverman, J. H. (1988). Computing heights on elliptic curves. *Mathematics of computation*, 51(183) :339–358.

[44] Silverman, J. H. (1990). The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of computation*, 55(192) :723–743.

[45] Silverman, J. H. (1994). *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[46] Tate, J. (1995). A review of non-Archimedean elliptic functions. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 162–184. Int. Press, Cambridge, MA.

[47] Taylor, R. and Wiles, A. (1995). Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics*, pages 553–572.

[48] The PARI Group (2019). *PARI/GP version `2.11.2`*. Univ. Bordeaux. available from `http://pari.math.u-bordeaux.fr/`.

[49] Van Der Put, M., Gekeler, E., Reversat, M., and Van Geel, J. (1997). *Drinfeld Modules, Modular Schemes And Applications*. World Scientific.

[50] Washington, L. (1987). Class numbers of the simplest cubic fields. *Mathematics of Computation*, 48(177) :371–384.

[51] Watkins, M. (2002). Computing the modular degree of an elliptic curve. *Experimental Mathematics*, 11(4) :487–502.

[52] Watkins, M. (2012). Some remarks on Heegner point computations. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 81–97. Soc. Math. France, Paris.

[53] Weil, A. (1970). On the analogue of the modular group in characteristic *p*. In *Functional analysis and related fields*, pages 211–223. Springer.

[54] Wuthrich, C. (2018). Numerical modular symbols for elliptic curves. *Math. Comp.*, 87(313) :2393–2423.

[55] Zagier, D. (1985). Modular parametrizations of elliptic curves. *Canadian Mathematical Bulletin*, 28(3) :372–384.

Annexe A

Programmes PARI/GP

A.1 Programmes pour la divisibilité d'un point

Étant donné une courbe elliptique ell, un point $P \in \text{ell}(\mathbb{Q})$, entier $l \geq 1$, et un entier lim la fonction `divisible_local` teste pour les nombres premiers p inférieurs à lim tels que $\overline{\text{ell}}(\mathbb{F}_p)$ est une courbe elliptique et tel que $l \mid r_p = \#\overline{\text{ell}}(\mathbb{F}_p)$, si $\frac{r_p}{\ell}\overline{P} \neq O$. Lorsque $\frac{r_p}{\ell}\overline{P} \neq O$ la fonction retourne 0 et elle retourne 1 sinon. Autrement dit, lorsque la fonction retourne 0, il n'existe pas de point $Q \in \text{ell}(\mathbb{Q})$ tel que $lQ = P$. Si la fonction renvoi 1 on ne peut rien conclure.

```
divisible_local(ell,P,l,lim)=
{
  my();
  forprime(p=2,lim,
           d=ellgroup(ell,p)[1];
           if(d%l==0,
               if(ellpow(ell,P*Mod(1,p),d/l)!=[0],
                  return(0)
                  )
              )
           );
  return(1)
  }
```

Pour des entiers $n \geq 1, t \neq 0$, et une borne b, la fonction `test_div` exécute la fonction `divisible_local` sur la courbe elliptique E et le point $(0, n^3)$, pour tout entier l inférieur à la borne calculée à l'aide de la minoration de Krir (1.13).

```
test_div(n,t,b)=
```

```
{
  my(ell,Brn);
  ell=ellinit([0,t,0,-n^2*(t+3*n^2),n^6]);
  Brn=sqrt(ellheight(ell,[0,n^3])/log(ell.disc)*110592);
  forprime(l=2,Brn,
           print1(l ", ");
           if(divisible_local(ell,[0,n^3],l,b)==1,
              return(-1)
              );
           );
  return(1)
}
```

A.2 Programmes pour le calcul de la paramétrisation modulaire

Soient p un nombre premier, $r \geq 1$, $n \geq 0$ un entier. La fonction `did` renvoie le plus grand entier s et le plus grand entier $k \in [\![0, p-1]\!]$ tels que $n \geq kp^{rs}$.

```
did(p,r,n)=
{
  s=0;
  k=0;
  s=floor(log(n+0.01)/log(p^r));
  k=floor(n/p^(r*s));
  return([k,s])
}
```

Soit p un nombre premier et $r \geq 1$, et $n \geq 0$ des entiers. Si $n = a_s p^{rs} + \cdots + a_1 p^r + a_0$ est l'écriture en base p de n, la fonction `bij` retourne le polynôme $b_s T^s + \cdots + b_0$ de $\mathbb{F}_{p^r}[T]$, où

$$b_i = \begin{cases} 0 & \text{si } a_i = 0, \\ a^{a_s} & \text{si } a_i \neq 0 \text{ et } r \geq 2, \\ a_s & \text{sinon,} \end{cases}$$

avec a un générateur de $\mathbb{F}_{p^r}^*$.

```
bij(p,r,n)=
{
  my(s,R);
  R=0;
  m=n;
```

```
  if(r==1,
     while(m>0,s=did(p,1,m)[2];
           k=did(p,1,m)[1];
           R=R+k*T^s;m=m-k*p^s;
           ),
     a=ffgen(p^r,'a);
     R=0;
     m=n;
     while(m>0,s=did(p,r,m)[2];
           k=did(p,r,m)[1];
           R=R+a^k*T^s;m=m-k*p^(r*s);
           );
     );
  return(R)
}
```

La fonction `act` prend en entrée une matrice $M \in \mathrm{Gl}_2(K_\infty)$ et un élément $x \in \overline{\Omega}$ et renvoie l'élément Mx.

```
act(M,x)=(M[1,1]*x+M[1,2])/(M[2,1]*x+M[2,2])
```

Pour p un nombre premier et $r \geq 1$ un entier, la fonction `gl2` retourne l'ensemble des matrices de $\mathrm{Gl}_2(\mathbb{F}_{p^r})$.

```
gl2(p,r)=
{
  my(M);
  R=Mat();
  if(r==1,
     forvec(X=[[0,p-1],[0,p-1]],
            forvec(Y=[[0,p-1],[0,p-1]],
                   M=matconcat([X,Y]~);
                   if(matdet(M)*Mod(1,p)!=0,
                      R=matconcat([R,M])
                      );
                   );
            ),
     a=ffgen(p^r,'a);
     forvec(U=[[0,p^r-1],[0,p^r-1]],
            if(U[1]==0,
               x1=0,
               x1=a^U[1]
               );
            if(U[2]==0,
               x2=0,
               x2=a^U[2]
               );
            X=[x1,x2];
            forvec(V=[[0,p^r-1],[0,p^r-1]],
```

```
                    if(V[1]==0,y1=0,y1=a^V[1]);
                    if(V[2]==0,y2=0,y2=a^V[2]);
                    Y=[y1,y2];
                    M=matconcat([X,Y]~);
                    if(matdet(M)*Mod(1,p)!=0,
                       R=matconcat([R,M])
                       );
                    );
            );
  );
  return(R)
}
```

Étant donné un nombre premier p, un entier $r \geq 1$, un polynôme $N \in \mathbb{F}_{p^r}[T]$, un élément v de N^2 et $k \in \mathbb{N}$, la fonction `Matgive` construit une matrice de $\Gamma_0(N)$ avec la propriété : lorsque v parcourt $\mathbb{N}^2$ et k parcourt $\mathbb{N}$ cette matrice parcourt l'ensemble des matrices de $\Gamma_0(N)$ de déterminant 1.

```
Matgive(N,v,k,p,r)=
{
  my(P,Q,R,S,b);
  R=bij(p,r,v[1])*N;
  S=bij(p,r,v[2]);
  if(poldegree(gcd(R*Mod(1,p),S*Mod(1,p)))==0,
     b=gcdext(R,S);
     P=(b[2]-R*bij(p,r,k));
     Q=-(b[1]+S*bij(p,r,k));
     M=[P,Q;R,S]*Mod(1,p),
     M=[0,0;0,0]
     );
  return(M)
}
```

Étant donnés un nombre premier p, un entier $r \geq 1$, A une matrice de $\overline{\Gamma}$ et un point $z \in \overline{\Omega}$, la fonction `u` calcule le produit partiel de $u_\alpha(z)$ sur l'ensemble des matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}_0(N)$ telles que $\deg(c) \leq m$, et telles que $a = a_0 + Qc$, $b = b_0 + Qd$ avec $\deg Q \leq n$ et (a_0, b_0) le couple tel que $a_0 d - b_0 c \in \mathbb{F}_q^*$ construit avec l'algorithme d'Euclide étendu en choisissant comme point de base ω, une racine de P dans $\overline{K_\infty}$.

```
u(A,P,N,m,n,p,r,z)=
{
  my(M,G,D,s,d,b,dm,t);
  t=1*Mod(1,p)*Mod(1,P);
  a=ffgen(p^r,'a);
```

```
  d=0;
  b=p^(r*poldegree(N));
  forvec(w=[[0,floor((m+1)/b)-1],[0,floor((m+1)/p^(2*r))]],
         if(d<=w[1],print(d);d=d+1);
             for(k=0,n,
                 M=Matgive(N,w,k,p,r);
                 dm=polcoeff(M[2,2],poldegree(M[2,2]));
                 if(matdet(M)!=0&&dm==1,
                    for(j=1,p^r-1,
                    if(r==1,G=M*[j,0;0,1],G=M*[a^j,0;0,1]);
                    s=(z-act(G,y))/(z-act(G*A,y))*Mod(1,p);
                    s=substpol(s,T,1/x);
                    s=taylor(s,x,10);
                    t=t*s
                    );
                 );
          );
     );
  return(t)
}
```

Étant donné un représentant $M \in \mathrm{Gl}_2(K_\infty)$ d'une classe de $\mathrm{Gl}_2(K_\infty)/\mathcal{Z}\,\mathrm{Gl}_2(O_\infty)$. La fonction `Somt` retourne le représentant de la classe de M appartenant au système de représentants du lemme 52.

```
Somt(M,p,r)=
{
  my(u,s,b);
  a=ffgen(p^r,'a);
  A=substpol(M,T,1/x)*Mod(1,p);
  if(valuation(A[2,1],x)<valuation(A[2,2],x),
     A=A*[0,1;1,0]
     );
  A=A*[1,0;-A[2,1]/A[2,2],1];
  A=A[2,2]^(-1)*A;
  b=A[1,1];
  s=valuation(b,x);
  u=b/x^s;
  A=A*[u^(-1),0;0,1];
  b=taylor(A[1,2],x,poldegree(A[1,1]));
  b=truncate(b);
  A=[A[1,1],b;A[2,1],A[2,2]];
  A=lift(A);
  return(A)
}
```

Étant donné une matrice $M \in \mathrm{Gl}_2(\mathbb{F}_{p^r}[T])$, $i \geq 0$ un entier, la fonction `Sommet` retourne le représentant de Mv_i appartenant au système de repré-

sentants du lemme 52.

```
Sommet(M,i,p,r)=
{
  my(u,s,b);
  a=ffgen(p^r,'a);
  mat=M*[T^i,0;0,1]*Mod(1,p);
  mat=substpol(mat,T,1/x);
  if(valuation(mat[2,1],x)<valuation(mat[2,2],x),
     mat=mat*[0,1;1,0]
     );
  print(mat);
  mat=mat*[1,0;-mat[2,1]/mat[2,2],1]*Mod(1,p);
  print(mat);
  mat=mat[2,2]^(-1)*mat;
  print(mat);
  b=taylor(mat[1,1],x,10);
  b=truncate(b);
  s=valuation(b,x);
  print(s);
  u=b/x^s;
  truncate(u);
  mat=[b,mat[1,2];mat[2,1],mat[2,2]];
  print(mat);
  u^(-1);
  mat=mat*[u^(-1),0;0,1];
  print(mat);
  b=taylor(mat[1,2],x,poldegree(mat[1,1]));
  b=truncate(b);
  mat=[mat[1,1],b;mat[2,1],mat[2,2]];
  mat=lift(mat);
  return(mat)
}
```

Étant donné un sommet $v = v(j,u) \in X(\mathcal{T})$, la fonction fonction `Returnmat` retourne le type i de v et une matrice M telle que $v = Mv_i$.

```
Returnmat(v,p,r)=
{
  my(m,y,P,s,u);
  a=ffgen(p^r,'a);
  s=0;
  u=0;
  A=[1,0;0,1]*Mod(1,p);
  M=[x^v[1],v[2];0,1]*Mod(1,p);
  y=M[1,2];
  m=v[1];
  while(s==0,
```

```
        P=0;
        if(m<1,P=substpol(M[1,2],x,1/T);
           M=[1,-M[1,2];0,1]*M;
           A=[1,-P;0,1]*A;
           s=1,
           for(k=valuation(M[1,2],x),0,
               P=P+polcoeff(M[1,2],k,x)*x^k
               );
           M=[1,-P;0,1]*M;
           P=substpol(P,x,1/T);
           A=[1,-P;0,1]*A;
           y=M[1,2];
           if(y==0,
              A=[0,1;1,0]*A;M=[0,1;1,0]*M;
              M=M*[0,1;1,0]*[x^(-m),0;0,x^(-m)];
              M=substpol(M,x,1/T);
              s=1,
              A=[0,1;1,0]*A;
              m=m-2*valuation(y,x);
              y=taylor(y^(-1),x,m);
              y=truncate(y);
              M=[x^m,y;0,1]*Mod(1,p);
              );
           );
        );
  M=substpol(M,x,1/T);
  M=matconcat([A^(-1),M]~);
  return(lift(M))
}
```

Étant donné un sommet $v \in X(\mathcal{T})$, la fonction `Somconnect` renvoie tous les sommets voisins de v dans $\mathcal{T}$.

```
Somconnect(v,p,r)=
{
  my(M,A,f);
  a=ffgen(p^r,'a);
  M=[x^v[1],v[2];0,1]*Mod(1,p);
  R=Mat();
  A=M*[0,1;x,0];
  A=Somt(A,p,r);
  R=matconcat([R,A]);
  if(r==1,
     for(k=0,p-1,
         A=M*[k,1;1,0]*[0,1;x,0];
         A=Somt(A,p,r);
         R=matconcat([R,A]);
         ),
     for(k=0,p^r-1,
```

```
          if(k==0,f=0,f=a^k);
          A=M*[f,1;1,0]*[0,1;x,0];
          A=Somt(A,p,r);
          R=matconcat([R,A]);
          );
      );
  R=lift(R);
  return(R)
}
```

Étant donné un sommet $v \in X(\mathcal{T})$, la fonction `Pathtozero` donne le chemin reliant v au sommet $v(0,0)$.

```
Pathtozero(v,p,r)={
my(M,d);
a=ffgen(p^r,'a);
if(valuation(v[2],x)>v[1],v[2]=0);
M=[x^v[1],v[2];0,1]*Mod(1,p);
R=Mat(M);
if(v[2]!=0,
   d=valuation(v[2],x);
   d=v[1]-d;
   print(d);
   for(k=1,d,M=M*[x^(-1),0;0,1];
       b=taylor(M[1,2],x,poldegree(M[1,1]));
       b=truncate(b);
       M=[M[1,1],b;M[2,1],M[2,2]];
       R=matconcat([R,["->";"->"],M]);
       ),
   d=0;
   );
while(M!=[1,0;0,1]*Mod(1,p),
      if(v[1]-d<0,M=M*[x,0;0,1],M=M*[x^(-1),0;0,1]);
      R=matconcat([R,["->";"->"],M]);
      );
return(lift(R))
}
```

Étant donné $n \in \mathbb{F}_{p^r}[T]$ et deux sommets $v, v' \in X(\mathcal{T})$ de type i, donnés par $v = Uv_i, v' = Vv_i$, la fonction `gamma_equiv` retourne l'ensemble des matrices $\gamma \in \Gamma_0(n)$ telles que $v' = \gamma v$.

```
gamma_equiv(U,V,i,p,r,n)=
 {
 my(A,B,b);
 a=ffgen(p^r,'a);
 S=Mat();
 if(i==0,M=gl2(p,r);
```

```
    for(j=1,matsize(M)[2]/2,
        A=vecextract(M,[2*j-1,2*j]);
        B=V*A*U^(-1)*Mod(1,p);
        if(B[2,1]*Mod(1,2)%n==0,S=matconcat([S,[B]]));
        ),
    for(k=0,p^r-1,
        if(r==1,b=k,if(k!=0,b=a^k,0));
        for(j=1,p^(i*r+1)-1,
            A=[1,bij(p,r,j);0,b]*Mod(1,p);
            B=V*A*U^(-1)*Mod(1,p);
            if(B[2,1]%n==0,S=matconcat([S,[B]]));
            );
        );
  );
S=lift(S);
return(S)
}
```

Titre : Points spéciaux et modularité des courbes elliptiques définies sur $\mathbb{Q}$ et $\mathbb{F}_q(T)$

Mots clés : courbes elliptiques, paramétrisation modulaire, courbes modulaires de Drinfeld.

Résumé : Dans cette thèse, nous travaillons sur deux problèmes indépendants. La première partie concerne l'étude d'une famille de courbes elliptiques définies sur $\mathbb{Q}$ à deux paramètres. Le résultat principal prouve la non-divisibilité d'un point générique sous certaines conditions.
Dans la seconde partie, nous nous intéressons à la paramétrisation modulaire sur les corps de fonctions par les courbes modulaires de Drinfeld. La construction de la paramétrisation due à Gekeler et Reversat dans ce contexte est plus complexe que dans le cas classique des courbes elliptiques définies sur $\mathbb{Q}$. Nous y déterminons une formule explicite sur l'image des pointes par la paramétrisation modulaire. Puis nous donnons une borne explicite sur l'ordre de l'image de ces pointes qui est fini d'après un résultat de Gekeler. Finalement, nous illustrons les résultats à travers deux exemples en caractéristiques 2 et 3 de courbes elliptiques avec des conducteurs de petits degrés.

Title : Special points and modularity of elliptic curves defined over $\mathbb{Q}$ and $\mathbb{F}_q(T)$.

Keywords : elliptic curves, modular parametrization, Drinfeld modular curves.

Abstract : In this thesis, we work on two independent subjects. The first is a study of a two-parameter family of elliptic curves defined over $\mathbb{Q}$. The main results asserts under mild conditions that a generic point belonging to the curve is not divisible.
In the second work, we are interested in the modular parametrization over function fields by Drinfeld modular curves. The construction of the modular parametrization due to Gekeler and Reversat in this context is more complicated than the construction in the classical case of elliptic curves defined over $\mathbb{Q}$. We determine an explicit formula on the image of cusps by the modular parametrization. Furthermore we know by a work of Gekeler that the image of a cusp has finite order. We give an explicit bound on its order. Finally we study two examples in characteristic 2 and 3 of elliptic curves with small degree conductors.